Ministerie van Defensie

Defensie High-Level IT-ontwerp

Datum	24 april 2015
Status	V1.4.0 - Definitief

Colofon

BS

CDS en HDBV

Plein 4

Postbus 20701

2500 ES Den Haag

Contactpersoon A. Nagtegaal

Inhoud

1. Inleiding

Defensie is in toenemende mate afhankelijk van informatietechnologie (IT). Moderne IT is cruciaal voor effectief en doelmatig functioneren van de krijgsmacht bij het ondersteunen van de commandovoering, operationele inzet, de bedrijfsprocessen, de communicatiemiddelen, bemande- en onbemande wapensystemen, inlichtingen etc. Defensie maakt deel uit van de informatiemaatschappij die wordt gedreven door de razendsnelle ontwikkelingen in de IT.

De IT-infrastructuur van Defensie bestaat uit verschillende onderdelen, zoals rekencentra, netwerken en kantoorwerkplekken. Op de IT-infrastructuur draaien de informatiesystemen, oftewel applicaties. Binnen de context van dit document noemen we dit de IT-toepassingen. Hiermee wordt bedoeld de toepassingen die voor medewerkers beschikbaar zijn om gegevens op te slaan, te raadplegen, te verwerken, te archiveren of om het nemen van beslissingen te ondersteunen. Met name in het operationele domein neemt het aantal en het belang van IT-toepassing in hoog tempo toe. Commandanten zien zich in toenemende mate geconfronteerd met snel veranderende omstandigheden, complexe situaties en inventieve tegenstanders. Het nemen van de juiste beslissing op het juiste moment vereist betrouwbare informatie. Niet alleen de betrouwbaarheid van informatie is een aandachtspunt, maar ook het vinden van de juiste informatie in grote gegevensverzamelingen. Beschikbare gegevens nemen in volume enorm toe en daarmee ook de behoeften de relevante gegevens terug te vinden en te integreren met informatie van bijvoorbeeld partners.

In de loop van 2014 heeft extern onderzoek aangetoond dat de IT-infrastructuur, met nadruk op de rekencentra, een aantal kwetsbaarheden heeft. Defensie loopt risico omdat de technische staat van de bestaande IT-infrastructuur te wensen over laat en daardoor de continuïteit onvoldoende is geborgd. De cruciale delen van de IT zullen daarom de komende jaren vervangen en gemoderniseerd worden.

Een nieuwe IT-infrastructuur opent de weg naar de invoering van moderne technologieën, zoals cloudoplossingen, virtualisatie en het aansluiten op marktconforme-, RIJKS- en NATO-standaarden. Defensie kan daardoor eenvoudiger samenwerken met partners. Ten slotte biedt de modernisering van de IT-infrastructuur een momentum om te starten met een platform voor innovatie van IT binnen Defensie, oftewel een slimme bundeling van een nieuw technisch platform en de technologische kennis vanuit Defensie, markt en partners om IT in te zetten als permanente *enabler* voor innovatie van de krijgsmacht als geheel.

Om richting te geven aan de ontwikkelingen van de IT binnen Defensie is in dit document het High Level IT Ontwerp opgesteld. Het beschrijft welke business effecten de IT moet bewerkstelligen of ondersteunen, welke kaders aan de IT worden gesteld en hoe in functionele termen de toekomstige IT eruit moet komen te zien. Het vormt de stip aan de horizon waar de IT zich naartoe ontwikkelt. Ieder jaar wordt bekeken of bijsturing nodig is.

Uit onderzoeken is gebleken dat Defensie de nieuwe IT niet kan realiseren zonder samenwerking met de markt. Om richting te geven aan deze samenwerking zijn ook hiervoor eisen, kaders en uitgangspunten geformuleerd. Deze geven aan op welke gebieden de samenwerking wordt aangegaan (scope), in welke vorm wordt samengewerkt (verantwoordelijkheidsverdeling) en aan welke eisen deze samenwerking moet voldoen. Dit vormt de stip aan de horizon waar de samenwerking met de markt zich naartoe beweegt. Ook hiervoor geldt dat ieder jaar wordt gekeken of bijsturing nodig is.

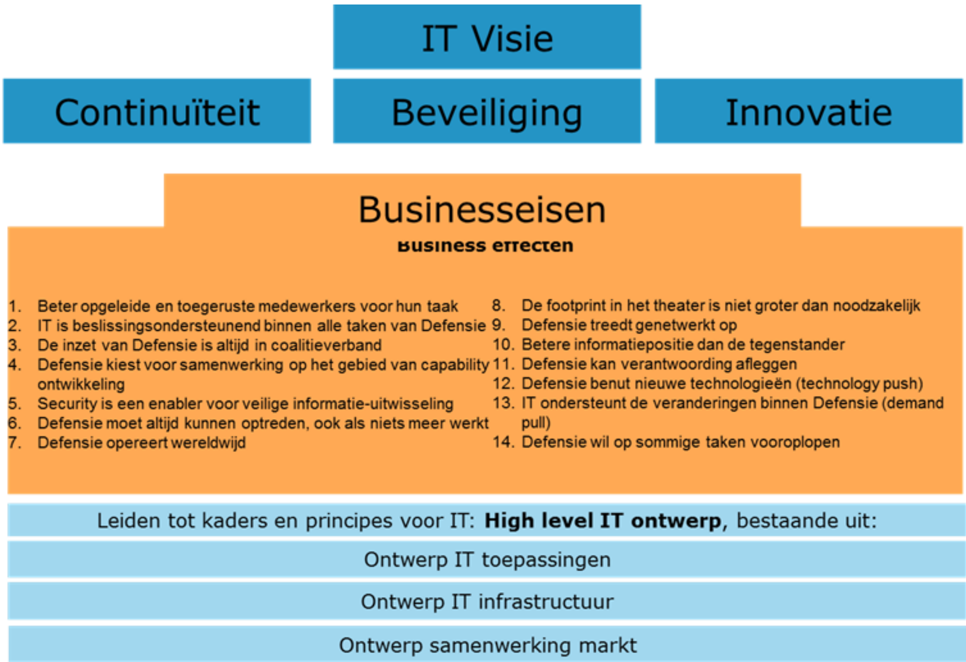
1.1 Samenhang

Het High Level IT-ontwerp is een vertaling van de noodzaak tot verandering die is ontstaan uit:

1. De Visie op IT.
2. De uitkomsten van de inventarisatie van de *business* eisen, vertaald in te realiseren *business* effecten.
3. De staat van de IT volgend uit het IT-assessment.
4. De identificatie van de cruciale processen uit het rapport van de *Business Continuïteit Management* (BCM).

De noodzaak tot verandering is in voorliggend document vertaald naar ontwerpprincipes: wat moet de IT bewerkstelligen, binnen welke kaders en in welke samenhang. Het vormt de stip aan de horizon. Weliswaar een stip die nooit helemaal stil zal staan, maar wel een die richting moet geven. Dit High Level IT-ontwerp dient als uitgangspunt voor het stappenplan waarin de opdrachten voor de realisatie worden aangegeven en in welke vorm de samenwerking met de markt wordt aangegaan (zie

Figuur 1).



Figuur 1. Samenhang

1.2 Leeswijzer

Hoofdstuk 2 vertaalt de beoogde *business* effecten in kaders waar de IT aan moet voldoen. Hieruit volgt de noodzaak tot verandering. Hoofdstuk 3 werkt de ontwikkelingen van de IT-toepassingen uit waarna hoofdstuk 4 het infrastructuurontwerp beschrijft. Hoofdstuk 5 bevat de belangrijkste verander- en migratieprincipes om de gewenst situatie te bereiken. Hoofdstuk 6 beschrijft hoe de samenwerking met de markt vorm moet krijgen om tot realisatie te komen. In hoofdstuk 7 wordt afgesloten met de conclusies.

2. Business effecten

2.1 Inleiding

De Visie op IT (referte 1) stelt dat IT een strategische *enabler* is waarvan de toekomst onmogelijk is te voorspellen. Defensie wil met IT daarom een ommekeer van denken en doen. Een onderdeel is dat de *business*, het militair optreden en bedrijfsvoering, leidend moet zijn. Daarom is aan de Defensieonderdelen en de MIVD gevraagd hoe hun onderdeel er in 2020 uitziet. De generieke karakteristieken zijn gebruikt om een beschrijving van de "Defensie van morgen" te maken.

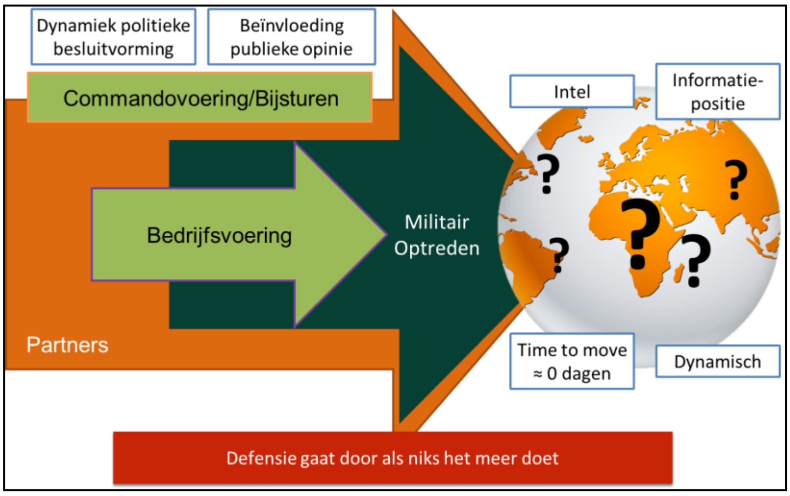
Defensie stuurt niet op de eventueel toekomstige technieken maar, conform de NEC-visie (paragraaf 2.3), op de effecten die Defensie wil bereiken. Dit document richt zich op de IT, echter Defensie dient ook de overige DCTOMP-factoren (Doctrine, Commandovoering, Training, Organisatie, Materieel en Personeel) hierop aan te laten sluiten om de gewenste effecten te bereiken. Defensie wil in bepaalde taken vooruit lopen. Deze taken zijn vooral te vinden in het militair optreden (inclusief het inlichtingenveld). Het militair optreden maakt veel gebruik van specifieke IT. Daarnaast moet het nieuwe innovatieplatform dit militair optreden gaan ondersteunen. De uitwerking hiervan vormt geen onderdeel van het HLO, maar door HDBV en CDS wordt in een overzichtsplaat inzichtelijk gemaakt wanneer welke IT wordt toegepast op basis van de Defensie *business capabilities*. Per *business capabilities* zal aangegeven worden of Defensie volgend is of juist voorop wil lopen.

De volgende paragrafen beschrijven zes business eisen. Deze business eisen representeren thema's waaruit kan worden afgeleid wat Defensie met IT wil bereiken (het effect). Hieruit komen de concretere eisen aan de IT voort. De zes thema's zijn:

- Business en mens staan centraal, IT sluit aan.
- De IT maakt veilig samenwerken in snel wisselende verbanden mogelijk.
- IT is betrouwbaar en beschikbaar.
- Met IT is Defensie 'wereldwijd *connected*'.
- De IT is geschikt voor verwerken, opslaan en analyseren voor zeer grote hoeveelheden informatie.
- De IT is eenvoudig en snel aanpasbaar.

2.2 Defensie van morgen

De toekomst is onzeker. De ontwikkelingen in de wereld veranderen steeds sneller. Daarnaast wordt Defensie blijvend geconfronteerd met de steeds maar sneller gaande technologische ontwikkelingen en innovaties. Defensie moet op dit geheel kunnen anticiperen. Dit doet Defensie door onder andere samen te werken met partijen zoals coalitiepartners, industrie, ngo's en overheden. Hierbij zijn de beoogde effecten, de samenstelling en bestaansduur per samenwerking anders.

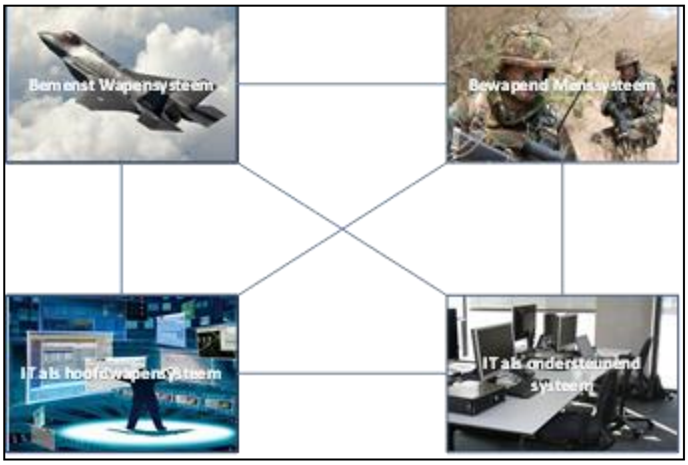


Figuur 2. Businesseisen: Defensie van morgen

Voor de interne samenwerking geldt daarnaast dat door de vergaande invoering van single service management, het militair optreden geheel afhankelijk geworden is van de bedrijfsvoering (zie Figuur 2). De dynamiek in het militair optreden is dus ook merkbaar in de bedrijfsvoering. CDC en DMO moeten daarom het militair optreden 24x7 wereldwijd ondersteunen.

Om de beoogde effecten en doelen te bereiken is actuele, tijdige en betrouwbare informatie een noodzaak. Door deze informatie en toegang tot deze informatie af te stemmen op de beoogde effecten en de omstandigheden waarin Defensie deze gebruikt, reduceert Defensie mogelijke fatale gevolgen van te veel aan informatie of het gebrek aan informatie. Communicatie blijft naast juiste informatie van cruciaal belang voor het bereiken van de beoogde effecten. Deze communicatie, welke IT voor het leeuwendeel ondersteund, tussen mensen, mens-machine en tussen machines onderling bestaat uit spraak, video en informatie en is afhankelijk van de beoogde effecten en omstandigheden wereldwijd inzetbaar.

Fundamenteel principe is dat de krijgsmacht zowel in Nederland als in buitenland moet kunnen optreden als "niets het meer doet". Als externe middelen niet meer beschikbaar zijn, moet de krijgsmacht beschikken over ondersteuning van de noodzakelijke, elementaire, informatievoorziening van de eigen middelen. Dit betreft minimaal spraak. Om dit zeker te stellen heeft de krijgsmacht verschillende typen IT-platformen: het bemenste wapensysteem, het bewapende menssysteem, IT als hoofdwapen en IT als ondersteunend systeem (zie Figuur 3).



Figuur 3. Platformen van de krijgsmacht

Via deze platformen krijgen de medewerkers van de krijgsmacht (direct, dan wel indirect) toegang tot de benodigde functionaliteit en informatie. Voorbeelden van de platformen zijn: de F35 en CV90 (bemenst wapensysteem), soldaat in theater (bewapend menssysteem), inlichtingensysteem (IT als hoofdwapensysteem) en ERP (IT als ondersteunend systeem). De medewerker van de krijgsmacht heeft, via de IT-platformen, toegang tot zijn/haar werkomgeving vanuit verschillende gebruiksomstandigheden (statisch, ontplooid, mobiel, uitgestegen of te voet). Elk van deze platformen kent specifieke behoeftes in de performance van de IT: een bemenst wapensysteem zal andere eisen aan bijvoorbeeld reactietijd stellen dan een ondersteunend systeem. De IT die de krijgsmacht nodig heeft dient zodanig flexibel te zijn dat de verschillende eisen en behoeftes ondersteund worden.

2.3 NEC Visie

Voor de Nederlandse krijgsmacht is *Network Enabled Capabilities* (NEC) het richtinggevende con-

cept. Doel is om tegen beheersbare kosten een flexibel en modulair inzetbare krijgsmacht op te bouwen en te onderhouden waarmee een geïntegreerde en gecoördineerde inzet van beschikbare capaciteiten wordt bereikt ten einde een hogere effectiviteit van het militaire optreden te bereiken. Het concept beschouwt militair vermogen - sensoren, effectbrengers (wapens), commandovoering-capaciteiten en ondersteunende capaciteiten - als een samenhangend maar flexibel samengesteld geheel, dat wordt ondersteund door één netwerk- en informatie-infrastructuur (NII) (zie Figuur 4). De NII is door Defensie verwoord in de Strategische Visie op de NII (referte 3). Daarmee ligt de basis voor netwerkend optreden in een veilige, robuuste en uitgebreide federatie van netwerken.



Figuur 4. De NEC-keten

Door een beter netwerk (IT-infrastructuur) is relevante informatie tijdig beschikbaar en kan tijdig gedeeld worden. Dit zal leiden tot een eenduidig en eenvoudig te interpreteren beeld en daarmee begrip van de situatie voor elk niveau; namelijk voor de individueel optredende militair, voor zijn commandant en voor de staf. Dit moet leiden tot een beter begrip van de situatie, betere besluitvorming, hoger tempo in de uitvoering van de acties en uiteindelijk resulteren in een betere effectiviteit van de missie, waarin het gewenste effect proportioneel en gesynchroniseerd is met de partners.

Dit ontwerp richt zich op de eerste twee stappen uit Figuur 4, te weten een beter netwerk (IT-infrastructuur) en betere informatie (IT-toepassingen). De keuzen in dit ontwerp zijn gebaseerd op de richting verwoord in de Visie op de IT (referte 1) en op de effecten die Defensie wil bereiken. Op basis van deze richtingen zijn de eisen aan de IT geformuleerd. Deze zijn in de volgende paragrafen beschreven. Zoals eerder vermeld, moet Defensie ook actie ondernemen op alle DCTOMP-factoren om de gewenste effecten te bereiken.

2.4 Business en mens staan centraal, IT sluit aan

Deze overkoepelende business-eis heeft consequenties voor de manier waarop de IT-architectuur gebouwd, geïmplementeerd, onderhouden en aangepast gaat worden. Defensie moet daarvoor een andere manier van denken en doen hanteren. De volgende business effecten (BE) moeten bij elk besluit en bij elke actie voorop staan.

Effect: Beter opgeleide en toegeruste medewerkers voor hun taak

De snelheid van opereren van Defensie vraagt ook om een korte inwerktijd van de medewerker. De verwevenheid van gereedstelling en inzet maakt dat het opwerken ook gedurende de inzet plaatsvindt. Simulatie maakt hier een belangrijk onderdeel van uit.

Capaciteit en kennis zijn schaars binnen Defensie en daarom dient de IT bruikbaar te zijn zonder een uitgebreide opleiding of instructie. Dat vereist een IT die intuïtief is en marktconform, het is bijvoorbeeld erg handig om de ervaring met een privé-device hier te gebruiken.

Marktconform houdt ook in dat er snel veranderingen in technologie kunnen optreden. Dit betekent voor de IT dat apparaatonafhankelijkheid nodig is.

Effect: IT is beslissingsondersteunend binnen alle taken van Defensie

IT verschuift van procesondersteunend naar beslissingsondersteunend. Dit laatste sluit aan op de dynamische wereld waarin Defensie zich begeeft.

IT moet de beoogde effecten/doelen, die op elk niveau binnen Defensie bestaan, tot op individueel taakniveau ondersteunen zodat de uitvoering ervan tijd- en plaatsonafhankelijk is maar wel afhankelijk is van de omstandigheden waarbinnen wordt gewerkt.

De IT moet optimaal passen bij de taak van de medewerker en de beslissingen die de medewerker moet nemen. Daartoe biedt de IT de mogelijkheden om flexibel informatie op te halen uit verschillende bronnen die voor de medewerker relevant zijn en kan de medewerker kiezen welke IT hij/zij op dat moment gebruikt om de beoogde effecten te bereiken.

Eisen aan de IT

- *BE1 - Intuïtief en vriendelijk in het gebruik*
  De middelen moeten in lijn zijn met de standaarden*, web-and-app*, in de markt die medewerkers kennen (app's, intuïtief, simpel in gebruik en laagdrempelig).
- *BE2 - Eenvoudig aanpasbaar voor de uit te voeren taak*
  IT moet alleen die informatie vragen/tonen die bij de taak en de uit te voeren activiteiten horen. IT verandert mee bij wijzigingen in taak, rol of omstandigheden van medewerker of wapensysteem. Het gebruik van standaard bouwblokken ondersteunt hierin.
- *BE3 - IT is beslissingsondersteunend*
  Geen knellend keurslijf dat te rigide is. IT is niet alleen een middel voor routinematige registratieve taken via vaste werkstromen, maar daarnaast vooral een slimme combinatie van procesondersteuning en beslissingsondersteuning waarbij mens en taak centraal staan.
- *BE4 - De IT voorziet in tijd-, plaats-, en device-onafhankelijk werken*
  Het gebruik van IT wordt niet belemmerd door tijd of locatie. Hiervoor ondersteunt de IT een breed scala aan (mobiele) communicatiemiddelen (wereldwijd).
- *BE5 - Beheeractiviteiten zijn op gebruikersniveau minimaal*
  Beheeractiviteiten aan IT worden voor de medewerker zoveel als mogelijk beperkt (medewerker wordt in principe niet belast met beheertaken). *Self-service* wordt mogelijk gemaakt wanneer dat de medewerker voordeel oplevert.
- BE6 - Medewerker*s beschikken over management en stuurinformatie die noodzakelijk is voor de taak*
  De IT voorziet in standaard management- en stuur-informatie. Daarnaast kunnen medewerkers zelf informatie aggregeren met standaard middelen uit bronnen waarvoor de medewerker geautoriseerd is.
- *BE7 - Elke medewerker en platform heeft een digitale identiteit*
  Medewerkers en platformen (zoals wapensystemen, IT-platformen, *IT-services* en *devices*) kunnen zich digitaal identificeren en hebben toegang tot informatie die de medewerker of platform nodig heeft voor de taakuitoefening. De rol van de medewerker/platform bepaalt de toegang tot de informatie.

2.5 De IT maakt veilig samenwerken in snel wisselende verbanden mogelijk

Effect: De inzet van Defensie is altijd in coalitieverband

De inzet van Defensie is altijd in coalitieverband. In inzet is de samenwerking *Joint, Interagency,*

Multinational, and Public (JIMP). Deze samenwerkingsvormen kent vele verschillende type externe samenwerkingen, bijvoorbeeld van vergaande strategische samenwerking tot ad hoc samenwerking. Maar ook samenwerking met partners die Defensie voor de missie vertrouwt maar in andere gevallen als tegenstander beschouwt.

Maar ook binnen Defensie is er intensieve samenwerking tussen de Defensieonderdelen. Defensie heeft het *single service management* ver doorgevoerd. Hierdoor is het militair optreden per definitie iets van meerdere Defensieonderdelen.

Effect: Defensie kiest voor samenwerking op het gebied van capability ontwikkeling

Defensie kiest voor samenwerking op het gebied van *capability* ontwikkeling (bundeling van krachten). Het gaat hierbij om intensivering van samenwerking met gelijkgestemde partners (nationaal en internationaal) en kennisinstituten. Het gaat daarbij niet alleen om samenwerking met andere krijgsmachten, maar ook samenwerking met civiele partners (ketenpartners, non-gouvernementele organisaties en de industrie) is noodzakelijk. Binnen de Rijksoverheid betreft dit vooral samenwerking met het Rijk, de OOV-sector, het ministerie van V&J en het ministerie van BZK.

Effect: Security is een enabler voor veilige informatie-uitwisseling

Samenwerken kan alleen als de participanten goed met elkaar kunnen communiceren en dat betekent in alle situaties dat informatie wordt uitgewisseld. Deze communicatie is niet alleen tussen mensen maar ook tussen mens-machine en machines onderling, bijvoorbeeld het gebruik van de sensoren van partners.

Het delen van informatie kan Defensie kwetsbaar maken. Het hebben van een superieure informatiepositie maakt het verschil in een conflict. *Cyber defence* capaciteiten garanderen de betrouwbaarheid van de informatie en de beschikbaarheid van de IT. Deze zijn bepalend voor een goede samenwerking met partners die veelal op vertrouwen is gebaseerd. Het selecteren en samenstellen van de juiste middelen en informatie om de beoogde effecten te bereiken wordt ondersteund door risicoreductie technieken waardoor mogelijke restrisico's en bijbehorende maatregelen zichtbaar worden.

Eisen aan de IT

- *BE8 - Defensie kiest voor IT die geschikt is voor federatieve samenwerking*
  In een federatief model houdt elke deelnemer controle over zijn eigen middelen. De middelen kunnen wel koppelen om informatie uit te wisselen en door middel van afspraken worden diensten aangeboden of afgenomen van elkaar. Hierbij volgt Defensie het concept van NAVO: *Federated Mission Network (referte 4)*.
- *BE9 - Defensie kiest voor IT die informatie-uitwisseling binnen Communities of Interest ondersteund*
  Binnen een *Community of Interest* (COI) geldt voor het uitwisselen en gebruiken van informatie het principe *Duty to Share*. Tussen verschillende COI's geldt het principe van *Need to Know*. De IT voorziet hierin door de rubriceringsniveaus transparant te maken voor de medewerker. De medewerker heeft toegang tot die informatie waarvoor hij geautoriseerd is.
- *BE10 - De IT biedt generieke koppelvlakken*
  Koppelen van processen over de grenzen van eenheden, processen of ketens heen wordt ondersteund met koppelvlakken die generiek zijn. De koppelvlakken zijn geschikt om binnen Defensie informatie tussen systemen uit te wisselen en buiten Defensie informatie uit te wisselen met partners of marktpartijen onder alle gebruiksomstandigheden.
- *BE11- Defensie neemt IT-maatregelen op basis van risicomanagement*
  De bedrijfsvoeringseisen bepalen het risicoprofiel waarop de benodigde beschikbaarheid, exclusiviteit en integriteit wordt bepaald. Informatie wordt beveiligd conform de bijpassende restricties. Dit wordt vastgesteld op basis van risicomanagement;
- *BE12 - Defensie houdt haar digitale weerbaarheid op peil*
  Om de inzetbaarheid van de krijgsmacht te waarborgen en haar effectiviteit te verhogen, versterkt Defensie de komende jaren haar digitale weerbaarheid. Met het oog op cyberdreiging voorziet de IT in maatregelen op het gebied van preventie, detectie en schadebeperking en het opleiden van medewerkers;

2.6 IT is betrouwbaar en beschikbaar

Effect: Defensie moet altijd kunnen optreden, ook als niets meer werkt

De gehele krijgsmacht is een 24-uurs organisatie die wereldwijd en dus in verschillende tijdszones inzetbaar is. De inzet van eenheden gebeurt steeds sneller met als uitgangspunt dat *time-to-move* ongeveer 0 dagen is. Ook in Nederland is de ondersteuning 24x7. De krijgsmacht moet kunnen optreden, ook als niets meer werkt, bijvoorbeeld als de publieke infrastructuren niet beschikbaar zijn. Dit geldt zowel in Nederland als in het buitenland.

Eisen aan de IT

- *BE13 - IT ondersteunt alle vormen van operationele inzet*
  IT moet dusdanig ingericht zijn dat deze alle vormen van optreden en samenwerkingsverbanden kan ondersteunen, binnen en buiten Nederland, voor alle hoofdtaken van Defensie. Dit betekent dat Defensie werkt met IT waarmee informatie met partners uitgewisseld kan worden, ook als regulier publieke communicatiemiddelen niet meer werken. Commandanten kunnen te allen tijde onderling communiceren.
- *BE14 - IT ondersteunt een continu, ononderbroken commandovoeringsproces*
  Commandovoering is een continu proces. Dit betekent dat IT een naadloze overgang ondersteunt tussen de verschillende fasen in commandovoering (besluitvorming en bevelvoering) en de eenheden die daarbij betrokken zijn.
- *BE15 - De IT garandeert adequate (end-to-end) informatiebeschikbaarheid*
  Het primaire proces is sterk afhankelijk van *end-to-end*-informatie waaronder ook de in-

formatie uit de ondersteunende processen. De IT integreert deze informatie over de hele keten van sensor naar effector onder alle omstandigheden (statisch, ontplooid, mobiel, uitgestegen en te voet).

- *BE16 - Voor de robuuste basis IT geldt het 'never out' principe*
  De IT moet zich gedragen als een NUTS-voorziening. Hiermee streeft Defensie dat IT altijd beschikbaar is. In die gevallen dat IT onverhoopt niet beschikbaar is, zijn continuïteitsplannen beschikbaar.
- *BE17 - IT ondersteunt graceful degradation*
  Ondanks dat Defensie streeft naar een IT die altijd beschikbaar is, houdt Defensie er rekening mee dat deze bij calamiteiten uit kan vallen. De IT moet dan in staat zijn om stapsgewijs uit te vallen. Commandovoering en wapensystemen worden als essentiële taak te allen tijde ondersteund.

2.7 Met IT is Defensie 'wereldwijd connected'

Effect: Defensie opereert wereldwijd

De IT zorgt ervoor dat Defensie wereldwijd kan communiceren en toegang heeft tot publieke en private netwerken. Daartoe bevat de IT voorzieningen om wereldwijde verbindingen te kunnen opbouwen tussen Nederland en inzetgebieden aan wal, in de lucht en op zee. Tevens kunnen IT-voorzieningen wereldwijde verbindingen opbouwen met partners. De verbindingen zijn dusdanig dat Defensie zowel gerubriceerde als ongerubriceerde informatie kan verzenden.

Effect: De footprint in het theater is niet groter dan noodzakelijk

Defensie wil de *footprint* in het theater verkleinen. Dit is enerzijds een kostenbesparende maatregel maar vooral een noodzaak. Het aantal specialisten is immers schaars. Om deze capaciteiten optimaal te benutten, dienen zij meerdere missies tegelijk te ondersteunen door middel van een *reachback*. Deze *reachback* is belangrijk voor het militair optreden. Echter, de daadwerkelijke inzet mag niet afhankelijk zijn van deze *reachback*. De afwezigheid van *reachback* kan wel grotere risico's betekenen bij het nemen van een beslissing.

Effect: Defensie treedt genetwerkt op

Defensie treedt genetwerkt op, echter het oppervlak van het theater waarin een eenheid optreedt, wordt steeds groter. Dit betekent enerzijds een loskoppeling van de sensor, *decisionmaker* en *shooter*. Hierdoor kan een eenheid/platform de sensor zijn, een andere eenheid/platform neemt de beslissing en weer een andere eenheid/platform vuurt dan af. Anderzijds betekent de vergroting van het oppervlak ook synchronisatie tussen de verschillende eenheden/platformen die op grotere afstanden in dezelfde operatie werken. De inzet is hiermee totaal afhankelijk van de verbindingen tussen deze eenheden en platformen. Daarom dienen deze altijd aanwezig te zijn.

Eisen aan de IT

- *BE18 - De IT levert wereldwijde verbindingen*
  De IT biedt middelen (*capabilities*) om wereldwijde verbindingen op te bouwen. Dit kunnen verbindingen zijn met eenheden op land, in de lucht of op zee. De informatie over deze verbindingen is voldoende beveiligd.
- *BE19 - De IT reduceert de footprint*
  Met IT zal Defensie haar footprint in inzetgebied kunnen verkleinen. Uitwisselen op basis van een gemeenschappelijke en uniforme IT-infrastructuur maakt mogelijk dat inlichtingen, sensorwaarnemingen vanuit (on)bemande systemen en door uitgestegen militairen decentraal en centraal (op afstand van het inzetgebied) combineerbaar zijn tot geïnte-

greerde informatie voor commandovoering en *situational awareness*.

- *BE20 - Er moet een gegarandeerde verbinding zijn tussen sensor-decisionmaker-shooter*
  In het theater moet een gegarandeerde verbinding zijn tussen *de sensor-decisionmaker-shooter*. Dit betekent een integratie van het wapensysteem met IT.
- *BE21 - IT toepassingen moeten militaire omstandigheden ondersteunen*
  Verbindingen zijn in operationele omstandigheden niet gegarandeerd aanwezig doordat Defensie bewust kan kiezen om deze af te sluiten (*black hole*) of door natuurkundige beperkingen. De IT toepassingen, gebruikt voor het militair optreden, moeten beschikbaar blijven.

2.8 IT verwerkt, slaat op en analyseert grote hoeveelheden informatie

Effect: Betere informatiepositie dan de tegenstander

Defensie wordt in toenemende mate geconfronteerd met de effecten van de digitalisering. Op het gebied van wapensystemen, *situational awareness* en inlichtingen is een enorme groei aan informatie zichtbaar en deze trend zal de komende jaren doorzetten. In de Defensie-industrie zien we een snelle ontwikkeling in bijvoorbeeld informatiesystemen voor commandovoering die verbonden zijn met bemande en onbemande wapensystemen.

Wapensystemen bevatten steeds meer informatietechnologie. Sensoren, IR en radar dragen in combinatie met open bronnen en inlichtingen bij aan een geïntegreerd omgevingsbeeld. De focus ligt op een betere informatiepositie dan de tegenstander en een ononderbroken en volledige *situational awareness*. Om *situational awareness* te kunnen leveren, zijn inlichtingen nodig. Het kunnen leveren van inlichtingen (verzamelen, analyseren, bewerken en verspreiden) kan alleen maar dankzij IT. IT is dan ook het hoofdwapensysteem voor inlichtingen.

Grote hoeveelheden informatie kunnen niet onbeperkt decentraal worden verwerkt en opgeslagen maar ook is het niet altijd mogelijk om de grote hoeveelheden informatie te transporteren naar een centrale verwerkingslocatie. De IT-infrastructuur is daarom geschikt voor zowel decentrale als centrale informatieverwerking. Er vindt een dynamische verdeling plaats van deze verschillende vormen van informatieverwerking afgestemd op de situatie en de behoefte.

Effect: Defensie kan verantwoording afleggen

De sterk toenemende hoeveelheid informatie moet in veel gevallen worden gearchiveerd. De tijdsduur en de manier van archiveren zijn afhankelijk van de eisen die wettelijke of anderzijds worden gesteld. Defensie moet verantwoording kunnen afleggen.

Eisen aan de IT

- *BE22 - IT ondersteunt centrale en decentrale informatieverwerking*
  De IT-infrastructuur is geschikt voor decentrale en centrale informatieverwerking. Er vindt dynamische verdeling plaats van deze verschillende vormen van informatieverwerking, afgestemd op de situatie en de behoefte.
- *BE23 - Onafhankelijk van de locatie is de informatie toegankelijk*
  Er is een balans tussen verbindingen en een verdeling tussen decentrale en centrale informatieverwerking om informatie wereldwijd toegankelijk te maken ongeacht de locatie.
- *BE24 - IT ondersteunt het analyseren van grote hoeveelheden informatie*
  IT ondersteunt het analyseren van grote hoeveelheden informatie die afkomstig is uit verschillende bronnen zoals sensoren, open bronnen en inlichtingen.
- *BE25 - IT ondersteunt archivering van de broninformatie*

> Voor het afleggen van haar verantwoording, dient Defensie de gebruikte broninformatie te archiveren. Dit is de informatie die gebruikt is voordat het bewerkt en/of geanalyseerd is.

2.9 De IT is eenvoudig en snel aanpasbaar

Effect: Defensie benut nieuwe technologieën (technology push)

De krijgsmacht als geheel moet opereren in een blijvende dynamische wereld. In het bijzonder op het gebied van IT moet Defensie meebewegen met snel veranderende omstandigheden zowel politiek, militair, maatschappelijk als technologisch. Innovatie beperkt zich hierbij niet tot het geïsoleerd introduceren van nieuwe technologieën ter ondersteuning van de informatiebehoeften, maar vereist het onlosmakelijk inpassen daarvan in de operationele inzet, gereedstelling, commando- & bedrijfsvoering, opleiding en training. Defensie betreft de markt en kenniscentra bij innovatie.

Procedures en processen van financiële planning, besluitvorming en aanbesteding moeten passen bij een responsieve omgeving waarin verandering de norm is. De benodigde innovatieve kracht vereist betrokkenheid en moet een sterke focus krijgen bij de operationele eenheden en hun commandanten.

Effect: IT ondersteunt de veranderingen binnen Defensie (demand pull)

De IT moet flexibel zijn om zich aan te passen aan ontwikkelingen ex- en intern van Defensie en in staat zijn om veranderende doctrines te ondersteunen en nieuwe technologieën te introduceren. Dit wordt bereikt door te kiezen voor een modulaire opbouw (bouwstenen). Tevens moet IT eenvoudig kunnen opschalen (bijvoorbeeld extra capaciteit bij plotselinge operationele noodzaak). De snelle veranderingen in de IT kunnen betekenen dat tegelijk meerdere versies operationeel als gevolg van de doorlooptijd van invoering.

Effect: Defensie wil op sommige taken vooroplopen

Op de meeste processen zoals materieellogistiek of financiën volgt Defensie andere partijen zoals de markt of andere krijgsmachten. Elk Defensieonderdeel heeft echter één of meerdere domeinen waarin zij voorloper wil zijn ten opzichte van mogelijke tegenstanders en partners. Dit zijn de domeinen waarin Defensie bewust innoveert.

Eisen aan de IT

- *BE26 - De IT is een enabler voor innovatie van de krijgsmacht*
  Door middel van *Concept Development and Experimentation* (CD&E) wordt de toegevoegde waarde van nieuwe mogelijkheden aangetoond en de medewerkers gestimuleerd tot duurzame verbetering van operationeel optreden, commandovoering, bedrijfsvoering, doctrines en opleidingen. De operationele eenheden en hun commandanten zijn hierbij nauw betrokken. Maar ook intensieve samenwerkingsverbanden met kenniscentra en de industrie worden opgebouwd om de IT voortdurend te innoveren.
- *BE27 - De IT is designed-to-change*
  De schaalbaarheid wordt bereikt door te kiezen voor een modulaire opbouw op basis van bouwstenen die standaard uit de markt worden onttrokken en onderling koppelbaar. De bouwstenen kunnen worden uitgebreid (opschalen) of worden afgebouwd (afschalen) en zijn eenvoudig aanpasbaar aan veranderende eisen of omstandigheden. De architectuur (samenhangende ontwerpstructuur) om bouwstenen te ontwerpen en te koppelen wordt gebaseerd op standaarden van Rijksoverheid, NATO of markt. Procedures en processen zijn gebaseerd op *best practices* en kunnen voldoen aan korte reactietijden.
- *BE28 - Defensie beheert de IT professioneel*

De beheerprocessen worden ingericht conform marktconforme standaarden en *best practices*. Het beheer beschikt over *tooling*, oftewel middelen om het beheer te ondersteunen. Beheer is zoveel mogelijk geautomatiseerd en vindt centraal plaats. Tijdens militaire acties worden lokaal geen IT-wijzigingen doorgevoerd. Defensie beschikt altijd over voldoende eigen capaciteit om de instandhouding tijdens operationele inzet te garanderen.

- *BE29 - Defensie beheert de IT volgens Life Cycle Management*
  De IT moet betaalbaar zijn en tevens technisch op peil worden gehouden. Dat vereist *Life Cycle Management* over de objecten in het IT-domein. Borgen van betaalbaarheid vereist dat kosten (investeringen en exploitatie) transparant moeten zijn. Onderdeel van *Life Cycle Management* is het *Lifecycle Cost Management*.
- *BE30 - De IT is wendbaar*
  Focus op kort cyclische, evolutionaire doorontwikkeling. Nieuwe technologische ontwikkelingen en kansen worden snel ingezet en benut.

2.10 Noodzaak tot veranderingen

De business eisen en effecten staan niet op zichzelf. Deze zijn mede ingegeven door overkoepelende trends zoals de ontwikkeling van de informatiemaatschappij en de behoefte om netwerkend op te treden. Dit vereist een nieuwe invulling van IT die duidelijk anders is dan de huidige.

2.10.1 Technische achtergrond bij de noodzaak tot verandering

De verschillende krijgsmachtdelen hebben in het verleden autonoom IT ontwikkeld of gekocht waardoor sprake is van een “lappendeken” om vergelijkbare taken te ondersteunen. Veel van deze IT is ontwikkeld met inmiddels verouderde technologie en niet flexibel genoeg om nog te worden aangepast of het is economisch onrendabel.

Knelpunt is dat deze verouderde IT in toenemende mate een *disabler* voor de bedrijfsvoering en de operationele inzet is. Vooral op het gebied van koppelbaarheid is de huidige IT beperkend en dat zal de door Defensie beoogde netwerkbenadering bij operationeel optreden op termijn onmogelijk maken. De sensoren in nieuwe wapensystemen leveren ook steeds meer informatie die ingebed moet worden in commandovoeringsprocessen. De huidige IT is daarvoor niet flexibel genoeg.

Het gezien het ambitieniveau van onze krijgsmacht onontkoombaar dat IT wordt opgezet die toegepast kan worden in de verschillende omstandigheden zodat de beoogde effecten en doelen maximaal worden ondersteund. Noodzakelijke wijzigingen in het totaal aan IT-systemen worden steeds frequenter en fijnmaziger. Denk bijvoorbeeld aan het verschil in IT-systemen en informatiebehoefte van een militair binnen de poort en van dezelfde militair buiten de poort. Dit geldt ook voor het analyseren van grote hoeveelheden informatie waarbij alleen tijdens de analyse zelf veel rekencapaciteit nodig is, die vervolgens vrijkomt voor andere activiteiten.

2.10.2 Netwerkbenadering ondersteunen

De bestaande IT ondersteunt het digitaal samenwerken, zeker met externe partijen, nauwelijks. De externe samenwerkingen die IT ondersteunt, zijn specifieke IT-oplossingen. Gevolg is dat medewerkers naar andere oplossingen zoeken om samen te werken. Hierdoor loopt Defensie beveiligingsrisico’s.

Defensie kiest voor de netwerkbenadering bij militair optreden. Het succes van de inzet van Nederlandse militairen is daarbij in grote mate afhankelijk van het vermogen tot samenwerken met andere krijgsmachtsonderdelen, andere landen en civiele partijen. Op het niveau van ingezette eenheden moeten C2-toepassingen, wapensystemen en sensoren zijn gekoppeld. Hierdoor is ieder wapen- of sensorsysteem ook IT en vervaagt het onderscheid tussen IT voor ondersteuning en IT

voor operationele inzet.

Dit vereist een IT die samenwerkingsverbanden meer stimuleert door het introduceren van zogenaamde *communities of interest* (COI). Hierbinnen is voor dit samenwerkingsverband, de noodzakelijke middelen, informatie en bescherming geregeld en waarbij de keuze en samenstelling van de IT-systemen in evenwicht is met de beoogde effecten (doelen) die bereikt moeten worden en de risico's die daarvoor genomen kunnen worden.

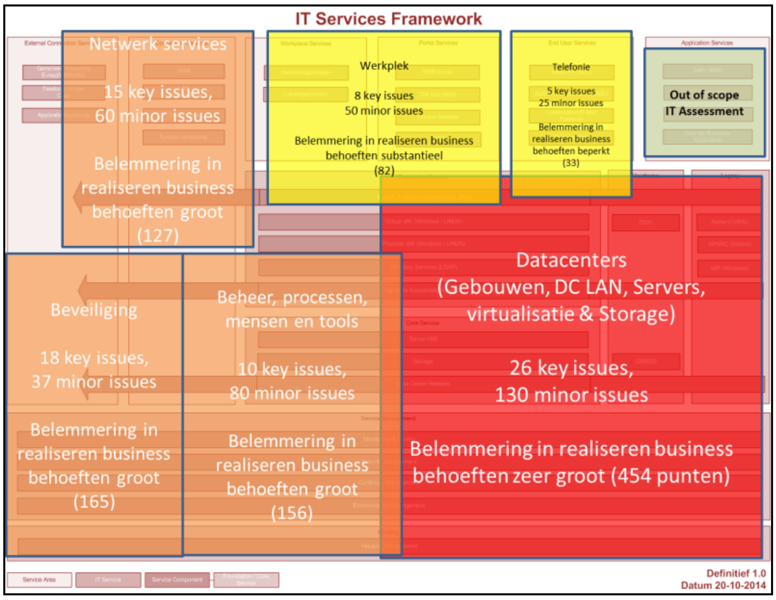
2.10.3 Flexibiliteit is cruciaal

Het is voor Defensie niet ongewoon om nieuwe IT te introduceren of aan te passen, maar het tempo waarin dit nu en in de toekomst moet gebeuren wel. De voorzienbare veranderingen in IT is onvergelijkbaar met de verandersnelheid in het verleden. Hierdoor kan Defensie nieuwe technologieën die op de markt gewoon zijn, niet adopteren. Maar ook de veranderingen in het militair optreden en de bedrijfsvoering kan de huidige IT niet ondersteunen. Als Defensie er niet in slaagt zich aan te passen aan de hoge verandergraad van IT, dan is informatiedominantie in het operationele domein niet realiseerbaar. De tegenstanders van Defensie volgen immers de veranderingen in de consumenten-industrie en zijn, niet gehinderd door beveiligingsaspecten of privacywetgeving, volledig flexibel in de keuze van technologie.

Defensie dient daarom kleine, zeer snelle en frequente stappen te zetten om veranderingen binnen de IT te realiseren, waardoor deze sneller en met minder technische en financiële risico's beschikbaar komt. Door een juiste mix van interoperabiliteit en modulariteit van de technische componenten worden deze ontwikkelingen en innovaties snel opgenomen in de IT van Defensie

2.10.4 IT infrastructuur moderniseren

Als deze eisen aan de IT worden gesteld, dan kunnen die veelal niet met de huidige IT infrastructuur gerealiseerd worden. De conclusie is dat alle IT services dienen te worden vernieuwd op basis van de uitgevoerde assessment. Vanuit het technologisch perspectief vormen de huidige datacenters, in de volle breedte, de grootste belemmering voor de krijgsmacht om invulling te geven aan de nieuwe IT visie. Figuur 5 bevat een schematische weergave.



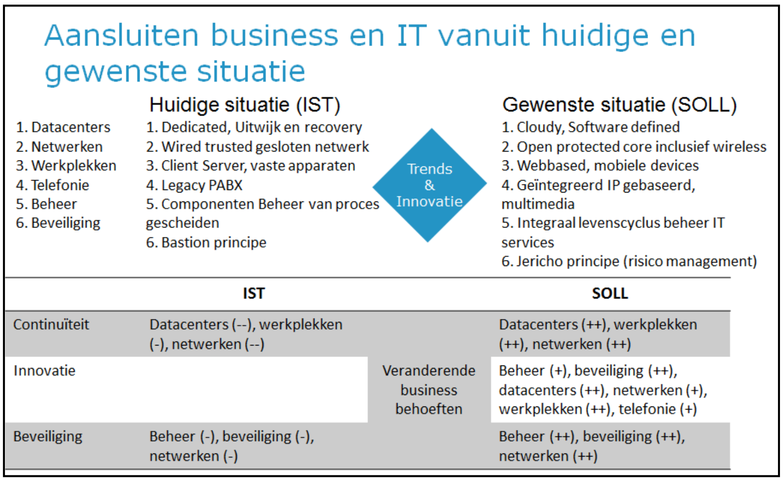
Figuur 5. Inventarisatie uitdagingen IT Services Framework

<u>Trends en ontwikkelingen</u>. Werken in de *cloud* en met het *web* en *apps* is de standaard in de civiele wereld en dat is ook het toekomstbeeld voor Defensie. Draadloze mobiele communicatie en *al-*

ways-connected is de standaard aan het worden met een grote diversiteit aan eindgebruikersapparatuur. Maar dan in alle gebruiksomstandigheden en voor alle rubriceringsniveaus (HLSOMUT). Het moet voor gebruikers gemakkelijk zijn om nieuwe functionaliteit (*apps*) te kunnen toevoegen. Voor de IT is de flexibiliteit en veranderbaarheid de succesfactor, zonder onaanvaardbare concessies op het gebied van veiligheid en betrouwbaarheid.

Belemmeringen. De huidige IT infrastructuur kent een groot aantal belemmeringen in het realiseren van de business behoeften van de komende jaren, zoals geïdentificeerd in het business spoor. Deze belemmeringen bevinden zich in de gehele keten van de IT infrastructuur. Dit is bevestigd door externe onderzoeken en de IT *assessment*. De belemmeringen worden veroorzaakt door:

- Verouderde infrastructuur met een verwevenheid van *legacy* applicaties.
- Sterke verwevenheid van de applicaties met het eindgebruikersapparaten (*devices*).
- Een netwerkvoorziening die voornamelijk gebaseerd is op een bedrade situatie. De gebruikers zijn in toenemende mate mobiel. Dit vereist draadloze communicatievoorziening en het kunnen gebruiken van mobiele *devices*.
- Het ontbreken van koppelingen met externe partners en tussen verschillende gebruikersdomeinen binnen Defensie.
- Ontbrekende functionaliteiten, dan wel functionaliteiten die niet over alle gebruikersomstandigheden (SOMUT) keten breed zijn te gebruiken en samenwerking belemmeren.
- Het ontbreken van een integrale vastgestelde architectuur met bijbehorende werkwijze. De operationele en niet-operationele IT en de IT voor de veiligheids- en inlichtingendienst zijn naast elkaar ontstaan en kennen hun eigen ontwerp. Dit terwijl de grenzen tussen generieke en specifieke IT in snel tempo vervagen.
- De beveiliging is primair gericht op het system *high bastion* concept dat belemmerend werkt in het samenwerken met partners en tussen verschillende gebruikersdomeinen binnen Defensie.
- De strikte scheiding tussen rubricerings- en securitydomeinen bemoeilijkt het werken.
- Het MUT (Mobiel, Uitgestegen, Te voet) domein loopt sterk achter op de overige netwerkvoorzieningen (niet interoperabele apparatuur, beperkte bandbreedte en verouderde communicatietechnologie).
- Beheertools en processen die zijn gericht op instandhouding van "spullen" en niet op continue vernieuwing van de IT-dienstverlening. Dit uit zich ook in de *skills* en mentaliteit van het betrokken personeel.
- Lange doorlooptijden om nieuwe functionaliteit te realiseren.



Figuur 6. Aansluiten business en IT vanuit huidige naar gewenste situatie

Uitgaande van de samenhang van de knelpunten en de benodigde veranderingen voor de SOLL situatie op basis van de trends en markt ontwikkelingen is doorgaan op de huidige weg geen optie, maar moet een vernieuwing uitgevoerd worden. Figuur 6 is een schematische weergave vanuit de huidige naar gewenste situatie. Belangrijke gegeven is dat "pleisters blijven plakken beslist niet leidt tot de gewenste resultaten. Dit verlengt alleen de instandhouding van de huidige situatie, maar biedt geen vernieuwing en innovatie en lost de uitdagingen niet op.

2.10.5 Samengevat

De huidige IT van de krijgsmacht sluit niet aan bij de behoefte. De huidige IT is om de volgende redenen niet geschikt om te voldoen aan deze behoefte en daarmee een *disabler* voor de toekomstige bedrijfsvoering:

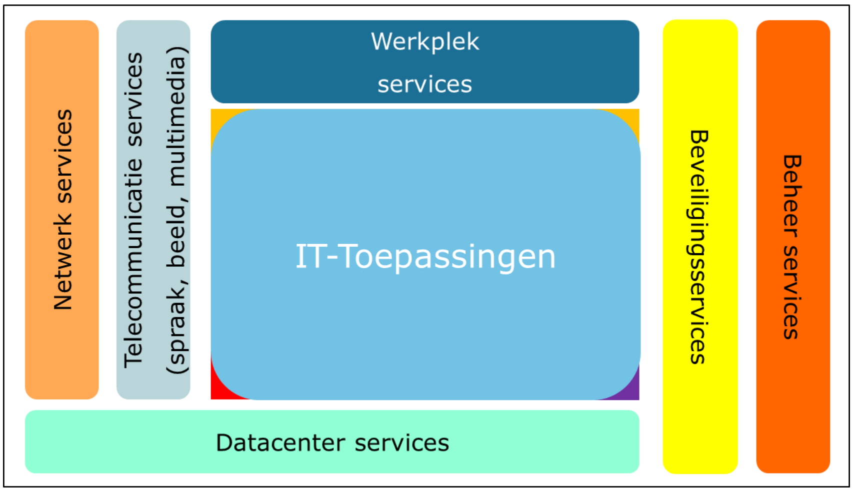
- De technische delen van de IT bestaan uit veel niet gestandaardiseerde bouwstenen van verschillende technologische generaties.
- Om informatiedominantie te behouden en te werken volgens de netwerkbenadering moeten systemen eenvoudig informatie kunnen uitwisselen en moet verandering een permanent proces worden. Een deel van de huidige IT dat wel nog voldoet aan moderne standaarden is niet altijd als zodanig ingericht dat veranderen eenvoudig kan.
- De generieke systemen, zoals ERP M&F en Peoplesoft zijn in de basis moeilijk veranderbaar en *build to last* (langdurig gebruiken, weinig veranderen). ERP M&F is juist bedoeld voor de relatief stabiele delen van de bedrijfsvoering.
- De specifieke systemen zijn deels verouderd en daarmee economisch of technisch niet meer verantwoord aan te passen (*end of life*).
- De IT is te sterk verdeeld in domeinen, waardoor de netwerkbenadering niet kan worden ondersteund. Het is complex om systemen onderling te laten communiceren in de mix van deels verouderde technologieën.

3. High Level Ontwerp IT-toepassingen

3.1 Inleiding

De noodzaak tot verandering, zoals geschetst in hoofdstuk 2, vertaalt zich naar eisen aan de nieuwe IT, bestaande uit de IT-infrastructuur en toepassingen. De nieuwe IT dient enerzijds betrouwbaar, veranderbaar en veilig te zijn. Ook moet invulling worden gegeven aan de eisen vanuit de bedrijfsvoering voor "Defensie van morgen". In dit hoofdstuk is de ontwikkeling van de IT-toepassingen geschetst. Paragraaf 3.2 bevat de huidige structuur aan de hand van het geheel aan de IT-toepassingen. Paragraaf 3.3 bevat de kaders en principes voor de gewenste situatie. In paragraaf 3.4 is ten slotte de gewenste structuur voor de toekomst op hoofdlijnen uitgewerkt.

Het onderscheid tussen IT-toepassingen en IT-infrastructuur is overeenkomstig de onderverdeling die rijksbreed gehanteerd wordt in de Enterprise Architectuur Rijk (EAR). De EAR maakt een onderscheid tussen applicatiediensten, werkplekservices, datacenter services, telecommunicatie services, netwerkservices en beheer- en beveiligingsservices. In dit rapport worden deze applicatiediensten de IT-toepassingen genoemd. Figuur 7 bevat een vereenvoudigde weergave van de Defensie architectuur die is gebaseerd op deze EAR-indeling.



Figuur 7. Vereenvoudigde impressie van de defensie architectuur

3.2 De structuur van het huidige landschap van IT-toepassingen (IST)

Defensie beschikt in de huidige situatie over een breed scala aan IT-toepassingen (applicaties). Het grootste gedeelte daarvan betreft losse toepassingen van vele verschillende leveranciers, vaak ontwikkeld of gekocht voor ondersteuning van specifieke taken, zoals commandovoering, inlichtingen, bediening van wapensystemen of administratieve taken. Daarnaast zijn er grote generieke toepassingen ter ondersteuning van de Defensiebrede (gestandaardiseerde en geïntegreerde) administratieve processen, met name de ondersteunende bedrijfsvoering. Voorbeelden zijn ERP, Peoplesoft en een aantal grote *legacy*-systemen.

In de toekomst zal er net als nu een tweedeling zijn in deze generieke en specifieke toepassingen van verschillende leveranciers. We noemen dit een hybride landschap van IT-toepassingen. Reden voor het behoud van een hybride landschap is dat er geen allesomvattende toepassing is en dat Defensie altijd wil kunnen kiezen uit de beste oplossingen die de markt biedt.

De kracht van het hybride landschap is dat Defensie de meest geschikte IT-toepassing kan gebruiken voor het vervullen van haar informatiebehoeften. Het hybride landschap heeft echter ook belangrijke beperkingen. Het is moeilijk veranderbaar, er zijn talloze complexe koppelingen en me-

dewerkers beschikken vaak alleen over gegevens binnen systeemgrenzen en moeten daardoor op verschillende toepassingen tegelijkertijd inloggen om informatie te verzamelen.

3.2.1 *De generieke IT-toepassingen*

Een aantal toepassingen die Defensie gebruikt is ook gangbaar buiten Defensie. Deze toepassingen worden generieke IT-toepassingen genoemd.

Een bepaald type generieke toepassingen die door Defensie gebruikt worden betreft de software die meerdere bedrijfsfuncties in één oplossing ondersteunt voor de planning en uitvoering van defensiebrede processen. ERP (SAP), Peoplesoft en een aantal *legacy* systemen zijn daarvan voorbeelden. Een kenmerk van deze toepassingen is de bedrijfsbrede uniformiteit en procesgestuurde opzet. Deze toepassingen vallen onder de zogenaamde bedrijfsvoeringssystemen. Met deze bedrijfsvoeringssystemen worden grote gegevensverzamelingen beheerd en bedrijfsbrede procesketens geïntegreerd en procesgestuurd ondersteund, waarbij alle gebruikers van deze systemen dezelfde gegevens delen. Voordeel is dat een deel van de processen geautomatiseerd plaatsvindt. Het verbruiken van goederen leidt bijvoorbeeld automatisch tot bestellen bij een leverancier. De processen met een voorspelbare en routinematige afloop worden geïntegreerd ondersteund. Dit versterkt de standaardisatie, uitvoerbaarheid en handhaafbaarheid van deze processen. De invoering van deze systemen vergt veel inspanning omdat zowel bedrijfsvoering als systeemfuncties op elkaar moeten worden afgestemd over de grenzen van organisatiedelen. Na de invoering zijn deze systemen doorgaans stabiel en is de verandergraad relatief laag. In deze generieke geïntegreerde bedrijfsvoeringssystemen heeft Defensie in de afgelopen jaren grote financiële investeringen gedaan en het is voorzienbaar dat een aantal van deze generieke toepassingen nog vele jaren deel zal uitmaken van de IT van Defensie.

In de kracht van de generieke geïntegreerde bedrijfsvoeringssystemen schuilt echter ook een zwakte, namelijk de complexiteit. Voor het beheer zijn deze systemen arbeidsintensief en slechts moeizaam te doorgronden als na de invoering aanpassingen nodig zijn. Ook voor de gebruikers zijn deze systemen complex en een verandering vereist telkens weer intensieve begeleiding van de werkvloer. Het is dus van belang het aantal aanpassingen van deze systemen in de toekomst laag te houden, zowel voor het beheer als voor het gebruik.

Generieke bedrijfsvoeringssystemen zijn vooral in de volgende domeinen toegepast:

- *Materieellogistiek en financiën*: hiervoor is de invoering van ERP M&F als generiek systeem een belangrijke basis voor de processen binnen ketenlogistiek, systeemlogistiek financiële administratie, verantwoording en controle. In deze domeinen treffen we naast ERP ook nog een breed scala van specifieke systemen aan voor factuurafhandeling, vraagvoorspelling, voorraadbeheer en onderhoud.
- *Personeel*: Het personele domein is ter ondersteuning van de personele processen en organisatiemanagement grotendeels afhankelijk van Peoplesoft als generiek systeem. Naast Peoplesoft kent dit domein ook specifieke systemen voor veteranen, communicatie, afhandelen van meldingen, salaris etc.
- *Medisch*: In het medisch domein zijn vele losse systemen aanwezig voor diagnose en ondersteuning van behandeling. Daarnaast zijn er centrale systemen voor dossiervorming en patiëntenlogistiek. Behandeling op afstand (TeleMedicine) neemt een grote vlucht evenals de geautomatiseerde ondersteuning van diagnose en behandelprocessen.
- *Besturen*: voor het genereren van managementinformatie zijn tools beschikbaar om informatie te aggregeren en presenteren. Tevens bevatten vele losse systemen eigen oplossingen om managementinformatie te genereren.
- *Basisgegevens*: De bedrijfsvoeringssystemen zijn een bron voor basisregistraties. Basisregi-

straties worden gebruikt om Defensiebrede gegevensverzamelingen te beheren met daarin de basisgegevens over personeel, organisatie, materieellogistiek, onderhoud en financiën.

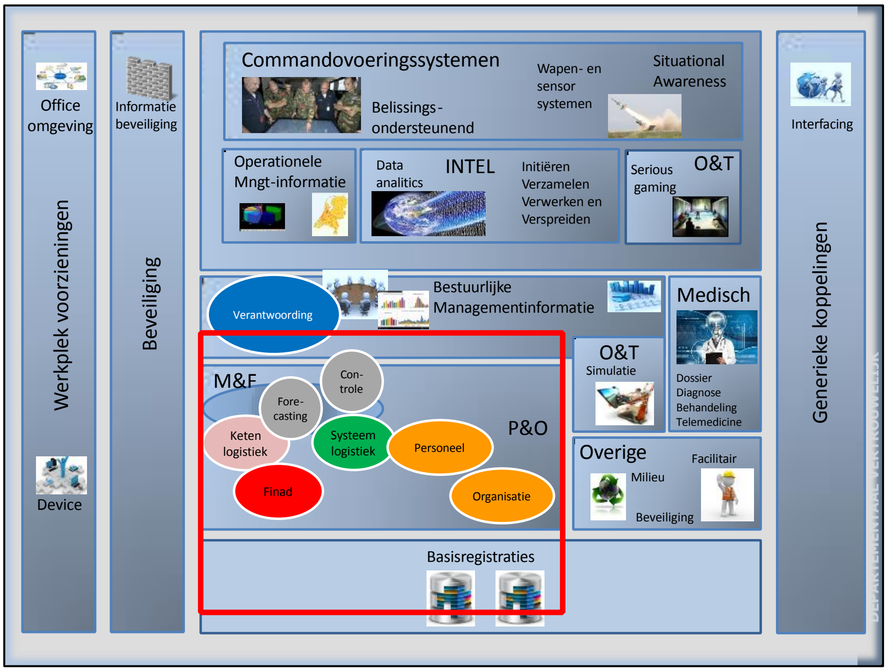
3.2.2 *De specifieke IT-toepassingen*

Naast generieke toepassingen beschikt Defensie over specifieke toepassingen die uniek zijn voor de krijgsmacht. Het betreft een grote diversiteit aan systemen, voor vele verschillende informatiebehoeften en niet geïntegreerde processen. Deze veelal losse IT-toepassingen, van verschillende technologieën en grote diversiteit komen voor in veel domeinen. Onderstaand een beknopte opsomming van de domeinen waarin deze specifieke toepassingen voorkomen:

- *Operationeel*. Voor operationeel optreden zijn verschillende oplossingen aanwezig voor beslissingsondersteuning, *situational awareness*, bediening van wapensystemen, communicatie tussen eenheden en connectie met partners. Zonder deze systemen is militaire inzet niet mogelijk.
- *Intel*. het Inteldomein is onderdeel van het operationele domein en beschikt over een breed scala van systemen ter ondersteuning van de inlichtingencyclus welke bestaat uit de fasen initiëren, verzamelen, verwerken en verspreiden. Intel is één van de *capabilities* die ingezet worden voor *situational awareness*. Daarnaast is er *reconnaissance*, *surveillance* en *target acquisition* (denk aan JISTARC).
- *Opleiding en training*: Defensie beschikt over systemen om opleidingsprocessen te ondersteunen, lesmaterialen te beheren en in toenemende mate over geautomatiseerde simulatie, *gaming* en trainingsfaciliteiten.

3.2.3 *Vereenvoudigd overzicht van het huidige landschap van IT-toepassingen (IST)*

Het geheel van generieke en specifieke systemen is het landschap van de IT-toepassingen binnen Defensie. In Figuur 8 is dit vereenvoudigd weergegeven. Het rood gemarkeerde deel bevat de domeinen met de belangrijkste bedrijfsvoeringssystemen. Dit is dus slechts een beperkt deel van het totale landschap.



Figuur 8. Impressie bestaand landschap van IT-toepassingen

Onder *overige* vallen toepassingen die ondersteunend zijn aan facilitair, milieu, veiligheid, commu-

nicatie, media etc. Dit is een breed scala van losse toepassingen voor verschillende, veelal gespecialiseerde processen. Overkoepelend aan de eerder genoemde domeinen beschikt Defensie over losse toepassingen om de werkplekvoorzieningen te ondersteunen. Dit betreft toepassingen voor mail, kantoorautomatisering (Office), samenwerkingsruimten, grafisch en procesontwerp.

In steeds meer situaties bestaat behoefte de gegevens uit verschillende toepassingen te combineren. Processen en informatiebehoeften stoppen niet bij de grenzen van een informatiesysteem waardoor toepassingen informatie moeten kunnen uitwisselen. Om de verschillende toepassingen met elkaar te verbinden maakt Defensie op dit moment gebruik van generieke koppelvlakken (GKD). Daarin bevinden zich verschillende oplossingen om toepassingen met elkaar te laten communiceren over de grenzen van technische omgevingen heen en over de grenzen van eerder genoemde domeinen heen. Daarnaast zijn er talloze directe koppelingen tussen toepassingen. Ten slotte zijn er voorziening om informatiebeveiliging te borgen conform de daarvoor geldende richtlijnen, kaders en wettelijke regels.

Informatiebeveiliging: Ten slotte zijn er voorzieningen om voor het gehele landschap van IT-toepassingen de veiligheid op orde te houden. In deze voorzieningen vinden we bijvoorbeeld oplossingen om de toegang tot informatie te regelen en gegevens te beschermen tegen ongeoorloofd gebruik.

3.3 Ontwerpprincipes voor het toekomstig landschap van IT-toepassingen

Met de mogelijkheden van de nieuwe IT-infrastructuur kan het complexe landschap van IT-toepassingen zodanig worden gemoderniseerd dat dit in stappen gaat aansluiten bij de *business eisen* en de Visie op IT.

Omdat deze situatie niet uniek is voor Defensie en ook binnen veel andere organisaties, zoals multinationals en grote dienstverleners, aan de orde is (vooral door opeenvolgende fusies), ontstaan vanuit de markt steeds meer moderne oplossingen om deze situatie het hoofd te bieden. De markt levert technologieën om verouderde en moderne IT-toepassingen beheersbaar te laten samenwerken, cruciale delen te hergebruiken en kwetsbare delen te isoleren (*designed to change*). Deze technologieën bieden ook oplossingen om de verouderde delen onzichtbaar te maken voor de gebruiker door deze te voorzien van een moderne schil waarmee de gebruiker interacteert. Het op een later tijdstip, in kleinschalige trajecten, saneren van de verouderde delen kan vervolgens zonder verstoring van het bedrijfsproces plaatsvinden en buiten het zicht van de gebruiker. Deze markt-technologieën vereisen echter een moderne IT-infrastructuur. De nieuwe IT-infrastructuur opent de weg om modernisering van dit complexe landschap door te voeren. Dit heeft tot gevolg dat voor de gebruikers van IT-toepassingen nieuwe, goedkopere en flexibelere oplossingen uit de markt bereikbaar zullen zijn, die zonder complexe ingrepen inpasbaar zijn. Steeds meer IT-toepassingen zijn als standaard services op de markt verkrijgbaar en voor Defensie zeer geschikt of eenvoudig geschikt te maken. Het ontwerp en de opbouw van de nieuwe IT-infrastructuur biedt derhalve een basis om het complexe landschap van IT-toepassingen van Defensie met kleinschalige, kort cyclische trajecten op orde te brengen en daarmee de flexibiliteit van de IT als geheel te verhogen en structureel kosten te besparen. Echter in een aantal gevallen is Defensie uniek. Ook dan is het verstandig eerst naar marktoplossingen te kijken. De situatie kan echter zo uniek zijn dat de markt geen afdoende oplossing biedt.

Om de *business* eisen te vertalen naar criteria om het systeemlandschap te moderniseren zijn ontwerpprincipes bepaald. Deze ontwerpprincipes zijn de kaders waaraan het toekomstig landschap van IT-toepassingen moet voldoen en zijn in lijn met de Visie van Defensie op IT en de *business* eisen uit hoofdstuk 2. De relatie tussen de deze ontwerpprincipes en de business thema's is opgenomen in bijlage 2 van dit document.

3.3.1 Ontwerpprincipes BE 1: Business en mens staan centraal, IT sluit aan

- *TP.01 IT-toepassingen zijn geschikt voor tijd-, plaats-, en device-onafhankelijk werken.*
  De toegang tot systemen wordt niet belemmerd door tijd of locatie. Tevens werken de systemen op een breed scala aan mobiele communicatiemiddelen (wereldwijd).
- *TP.02 De interactie tussen mens en systeem (userinterface) is afgestemd op de taak van de gebruiker of de rol in een proces en lijkt zoveel mogelijk op wat de medewerker op basis van marktproducten ook gewend is.*
  De interactie met IT-toepassingen past bij de taak die de medewerker uitvoert. De medewerker krijgt geen overbodige informatie gepresenteerd en hoeft geen onnodige handelingen te verrichten. De systemen zijn intuïtief, beslissingsondersteunend en kosten weinig inwerktijd en werken zoveel mogelijk conform de gebruiksstandaarden van de consumentenmarkt.
- *TP.03 Er is een beperkte mate van keuzevrijheid mogelijk voor de medewerker bij de interactie met IT-toepassingen.*
  De medewerker kan op persoonlijke apparatuur zelf IT-toepassingen (bijvoorbeeld *apps*) toevoegen en instellen, afgestemd op de eigen taak. De *apps* die informatie ontsluiten of informatie uit externe bronnen toegankelijk maken worden beschikbaar gesteld vanuit een "Defensie app-store" of binnen restricties vanuit publieke *app-stores*.
- *TP.04 Medewerkers beschikken over een uniforme digitale werkruimte.*
  De IT biedt de gebruiker een uniforme werkruimte waarmee hij/zij toegang krijgt tot de digitale wereld binnen en buiten Defensie.
- *TP.05 Alle Defensiemedewerkers krijgen een persoonsgebonden gebruikersaccount.*
  Iedere militair, burgermedewerker dan wel externe inhuur krijgt een persoonsgebonden gebruikersaccount dat is gebaseerd op de Basisadministratie Digitale Identiteit Defensie.
- *TP.06 Medewerkers beschikken over een digitale uitrusting.*
  De medewerker krijgt de middelen die nodig zijn voor het optimaal toepassen van IT binnen de toegewezen taak en/of functie.
- *TP.07 Basis voor het toegangsbeleid (access management) voor de IT-toepassingen is "role based access" en "context based acces".*
  De gebruiker heeft toegang tot het systeemlandschap met een vastgesteld gebruiksrecht dat is afgestemd op de taak die hem/haar is toegewezen. Bij de toewijzing van een taak beschikt hij/zij over de noodzaak en dus ook over de bevoegdheid om bepaalde systemen, services en gegevens te gebruiken en te raadplegen. Rollen worden ontleend aan vastgestelde criteria zoals functie, plaats in de organisatie, taken, positie, locatie, voorschriften en aanspraken van de medewerker (*claims of requests*). Het geheel aan rollen, regels en/of claims worden tevens gebruikt om bedrijfsregels met betrekking tot de toegang tot data en systemen vast te leggen en te verlenen. De context is eveneens bepalend voor de toegang tot informatie (situatie afhankelijke toegang tot gegevens).
- *TP.08 Commandovoeringssystemen ondersteunen alle missies.*
  De IT-toepassingen worden zodanig ingericht dat deze het proces van commandovoering in de krijgsmacht ondersteunen in alle vormen van optreden en samenwerkingsverbanden.

3.3.2 Ontwerpprincipes BE 2 - De IT maakt veilig samenwerken in snel wisselende verbanden mogelijk

- *TP.09 De IT-toepassingen brengen mensen veilig met elkaar in verbinding.*
  Om effectief te blijven zullen gebruikers van IT-toepassingen daarin de middelen aantreffen om teams met elkaar te verbinden, rekening houdend met de behoeften van doelgroepen (*com-*

munities of interest) en genetwerkt samenwerken (GSW). De IT-toepassingen voldoen aan de beveiligingseisen die Defensie stelt conform het informatiebeveiligingsbeleid van Defensie.

- *TP.10 IT-toepassingen zijn geschikt om informatie te delen en te integreren.*
  Over de hele keten van sensor naar effector kan onder alle omstandigheden (statisch, ontplooid, mobiel, uitgestegen en te voet) informatie worden geïntegreerd. Het primaire proces is sterk afhankelijk van geïntegreerde informatie uit meerdere bronnen (waaronder steeds meer sensoren), vooral om omgevingsbeeld op te bouwen en om beslissingen te nemen bij commandovoering. Daarbij is ook de informatie uit de ondersteunende processen en de informatie verkregen van partners (in federatie) van belang. Tevens moet Defensie de relevante informatie weer kunnen delen met en beschikbaar stellen aan partners.

- *TP.11 De beveiliging van IT (infrastructuur en toepassingen) is afhankelijk van het afbreukrisico.*
  Als niet wordt voldaan aan de eisen die gesteld worden aan de toegankelijkheid, vindbaarheid, uitwisselbaarheid, betrouwbaarheid, authenticiteit en volledigheid van de informatie dan worden keuzes van authenticatiemiddelen en beveiliging gebaseerd op afbreukrisico. Daarbij gelden de volgende criteria vanuit de informatiebeveiliging:
  a. Het risico wordt bepaald aan de hand van de bedrijfsvoeringseisen uitgewerkt in een risicoprofiel waarbij belang voor de bedrijfsvoering/operaties centraal staat.
  b. Het rubriceringsniveau en/of niveau van merking is bepalend voor de beveiligingseisen. Informatie wordt beveiligd conform de restricties die voor de betreffende gegevens van kracht zijn. Dit wordt vastgesteld op basis van risicomanagement.
  c. Om de inzetbaarheid van de krijgsmacht te waarborgen en haar effectiviteit te verhogen, versterkt Defensie de komende jaren haar digitale weerbaarheid. Met het oog op cyberdreiging voorziet de IT in maatregelen op het gebied van preventie, detectie en schadebeperking.
  d. Defensie conformeert zich aan marktstandaarden zoals ISO en kaders zoals bepaald in BIR, VIR, VIR-BI, Wet op de Staatsgeheimen, NAVO en EU-richtlijnen en houdt rekening met (recente) wettelijke kaders, zoals PIA en WBP en het Defensie beveiligingsbeleid van de SG. Defensie kan richting samenwerkingspartners aantonen in control te zijn en de afspraken nakomen.
  e. Medewerkers worden bewust gemaakt van hun eigen verantwoordelijkheden op het gebied van veiligheid en beveiliging.

3.3.3 *Ontwerpprincipes BE 3 - IT is betrouwbaar en beschikbaar*

- *TP.12 Het landschap van IT-toepassingen ondersteunt alle vormen van operationele inzet.*
  Het geheel van toepassingen wordt zodanig ingericht dat alle vormen van optreden inclusief de daarbij behorende samenwerkingsverbanden worden ondersteund, binnen en buiten Nederland, voor alle taken van Defensie.

- *TP.13 Het landschap van IT-toepassingen van Defensie is een hybride landschap.*
  Er is niet één allesomvattend systeem dat alle informatiebehoeften van Defensie invult. Het stelsel van IT-toepassingen is nu en in de toekomst een hybride stelsel van verschillende oplossingen en technologieën. De hybridestructuur bestaat uit een mix van procesondersteunende toepassingen en (kleinere) speciale IT-toepassingen met daaromheen flexibele oplossingen om IT te integreren en zodoende ononderbroken informatieketens te ondersteunen tot in het inzetgebied.

- *TP.14 De hybridestructuur werkt voor Defensie-brede processen als één samenhangend stelsel voor de informatievoorziening.*

Het landschap van IT-toepassingen bevat marktconforme tools om systemen zodanig te integreren dat voor de gebruikers een samenhangend stelsel ontstaat, voor die processen waarvoor dat gewenst is.

- *TP.15 De herkomst van de IT-toepassingen is divers.*
  Defensie maakt in de hybride structuur gebruik van oplossingen van verschillende partijen. IT-toepassingen komen van marktpartijen, Rijksoverheid, NATO, Defensie-industrie of in uitzonderlijk geval door eigen ontwikkeling.

- *TP.16 Voor veranderingen van IT-toepassingen geldt 'geen maatwerk'.*
  IT-toepassingen worden zoveel mogelijk *out of the box* ingericht (geen maatwerk) zodat beheeractiviteiten uitvoerbaar zijn volgens de standaard richtlijnen van de leverancier. Nieuwe IT-toepassingen worden ingevuld met standaard van de markt verkrijgbare oplossingen, zoals standaard services. De volgende voorkeursvolgorde geldt voor de selectie en implementatie van nieuwe delen:

  a. NATO-brede toepassingen.
  b. Rijksbreed generieke toepassingen.
  c. Bedrijfsproces generieke toepassingen.
  d. *Military of the shelf*.
  e. Standaard software, *commercial of the shelf* vanuit de markt.
  f. Maatwerk.

  Het beheren en inrichten van de *tools* om de verschillende IT-toepassingen te integreren wordt niet bij voorbaat beschouwd als ongewenst maatwerk. Het integreren van IT-toepassingen vraagt vaak om Defensie specifieke keuzes, evenals het beheren, implementeren en onderhouden van bedrijfsregels. Daarbij geldt wel dat de *tools* marktconform dienen te zijn.

  In het inteldomein, vooral voor de MIVD moet rekening worden gehouden met de samenwerking met de AIVD. Zo komt het regelmatig voor dat de JSCU (MIVD & AIVD) eigen toepassingen ontwikkelt (bijv. hack in het kader van Cyber). Ook begint in de intel-wereld het concept DevOps. Ondanks de keuze dat zoveel mogelijk van buiten Defensie wordt betrokken moet beperkte ontwikkelcapaciteit in de organisatie aanwezig zijn.
  Ook voor het invullen van specifieke wensen vanuit de operationele eenheden van Defensie kan het noodzakelijk zijn om in beperkte mate zelf te ontwikkelen. Redenen hiervoor kunnen zijn dat de markt geen passende oplossing kan bieden of niet kan voldoen aan bepaalde eisen in het kader van beschikbaarheid of betrouwbaarheid. Er zal derhalve beperkte eigen ontwikkelcapaciteit behouden blijven.

- *TP.17 Stamgegevens worden eenmalig opgeslagen en meervoudig gebruikt.*
  Data (stamgegevens) worden eenmalig opgeslagen en beheerd, maar zijn beschikbaar voor alle processen die deze data nodig hebben.

- *TP.18 De IT-toepassingen garanderen adequate informatiebeschikbaarheid voor commandovoering.*
  De IT-toepassingen voldoen aan de eisen ter bevordering van effectieve en efficiënte uitvoering van opdrachten op elk niveau en onnodige risico's voor het personeel en van het materieel worden geminimaliseerd.

- *TP.19 Commandovoeringssystemen ondersteunen een continu en ononderbroken proces.*
  De IT-toepassingen worden zodanig ingericht dat alle relevante informatie, voor de operationele inzet van militaire componenten, kan worden verzameld, geanalyseerd, verspreid, gebruikt,

geborgd en geëvalueerd. De IT ondersteunt hiermee de versterking van militair vermogen conform de uitgangspunten van *Network Enabled Capabilities*.

3.3.4 *Ontwerpprincipes BE 4 - Met IT is Defensie 'wereldwijd connected'*

- *TP.20 IT-toepassingen zijn geschikt om wereldwijd informatie uit te wisselen via gangbare militaire of publieke communicatiemiddelen.*
  De IT-toepassingen kunnen, afgestemd op taak of proces, informatie-uitwisseling ondersteunen in alle gevallen dat technische verbinding beschikbaar is. Als verbinding niet mogelijk is kunnen systemen tijdelijk *disconnected* functioneren. Lokale dataopslag is daarvoor toegestaan.
- *TP.21 IT-toepassingen zijn geschikt om statisch, ontplooid, mobiel, uitgestegen en te voet beschikbaar te worden gesteld (SOMUT).*
  IT-toepassingen zijn zodanig opgezet dat gegevens kunnen worden geraadpleegd en uitgewisseld onder alle SOMUT-omstandigheden. De IT-toepassingen kunnen daarbij omgaan met een mix van lokaal opgeslagen informatie en informatie welke via netwerkconnectiviteit wordt gedeeld.
- *TP.22 Commandovoeringsystemen vormen een gesloten keten.*
  De IT-toepassingen garanderen de mogelijkheden voor *end-to-end* communicatie onder alle gebruiksomstandigheden: statisch, *deployed*, mobiel, uitgestegen en te voet voor alle krijgsmachtsdelen.
- *TP.23 Commandovoeringssystemen voldoen aan alle gebruikersomstandigheden.*
  Defensie moet eenheden kunnen inzetten in omstandigheden waarbij openbare IT niet gebruikt kan worden. De IT-toepassingen moeten geschikt zijn tijdelijk zonder connectiviteit te functioneren (*disconnected*) of met een minimale bandbreedte. Daartoe is lokale dataopslag (ook op mobiele middelen) toegestaan binnen de geldende beveiligingskaders.

3.3.5 *Ontwerpprincipes BE 5 - verwerking, opslag, archivering en analyse van data*

TP.24 IT-toepasssingen zijn geschikt om met grote hoeveelheden gegevens om te gaan.
IT-toepassingen zijn geschikt om opslag, archivering, verwerking en analyse te accommoderen van grote hoeveelheden ongestructureerde en gestructureerde gegevens waaronder sensorinformatie. Er zijn specialistische toepassingen beschikbaar voor het opslaan, verwerken en analyseren van gegevens in een zodanig volume dat deze niet meer door reguliere databasemanagement-omgevingen beheerd kunnen worden en speciale voorzieningen vereisen. Verzamelingen met dit volume worden *big data* genoemd. In de IT-toepassingen wordt onderscheid gemaakt in het kunnen benaderen van de opslagvoorzieningen, *tools* om de data te analyseren en *tools* om de geanalyseerde data beschikbaar te stellen aan andere IT-toepassingen.

3.3.6 *Ontwerpprincipes BE 6 - IT is eenvoudig en snel aanpasbaar*

- *TP.25 Nieuwe delen van IT-toepassingen zijn modulair, schaalbaar en aanpasbaar (designed to change)*
  De IT-toepassingen bestaan uit zelfstandige delen (modulaire opbouw) die koppelbaar zijn en eenvoudig vervangbaar of aanpasbaar zijn aan veranderende taken, eisen of omstandigheden. De zelfstandige delen worden zoveel mogelijk Defensiebreed hergebruikt.
- *TP.26 Voor veranderingen in het landschap van IT-toepassingen geldt het principe 'kleinschalig en kort-cyclisch'.*
  Er wordt niet meer veranderd met langdurige (meerjarige) trajecten die gebaseerd zijn op een

toekomstige *end state*. Veranderingen binnen en buiten Defensie gaan snel en zijn onvoorspelbaar. Daarom wordt vanaf nu veranderd in kleine en kort-cyclische stappen. Na ieder traject wordt opnieuw beoordeeld welke vervolgstap gewenst is (*stepping stone* principe).

- *TP.27 Het systeemlandschap van de toekomst is een enabler voor innovatie.*
  Het systeemlandschap wordt zodanig ingericht dat dit geschikt is om nieuwe technologische ontwikkelingen te beproeven en na beproeving snel in te voeren.
- *TP.28 Nieuwe delen van IT-toepassingen maken gebruik van scheiding tussen presentatie, logica en data-laag, tenzij de standaard logica in een IT-toepassing is gebaseerd op best practices.*
  In de huidige structuur van het landschap van IT-toepassingen is de logica (stelsel van bedrijfsregels dat vastligt in systemen) grotendeels vastgelegd in de (grote) procesondersteunende systemen en in COTS-pakketten op basis van *best practices*. Indien deze logica voldoet dan zal deze binnen de standaardfunctionaliteit gebruikt worden totdat de IT-toepassing uitfaseert. Voor nieuwe delen van het landschap van IT-toepassingen geldt dat de logica zoveel mogelijk buiten de systemen ligt in aparte oplossingen om bedrijfsregels te beheren en veranderingen eenvoudiger te kunnen doorvoeren.
- *TP.29 Bij de selectie van nieuwe IT-toepassingen geldt 'buy before make'.*
  Uitgangspunt is om geen nieuwe delen van het systeemlandschap zelf te ontwikkelen en gebruik te maken van standaardoplossingen uit de markt.
- *TP.30 Nieuwe delen van IT-toepassingen dienen schaalbaar te zijn m.b.t. resources van onderliggende IT-infrastructuur.*
  Nieuwe delen van IT-toepassingen zijn geschikt om te draaien op een IT-infrastructuur waarin resources flexibel kunnen worden toegewezen.
- *TP.31 Nieuwe delen van IT-toepassingen zijn geschikt om te worden aangeboden aan gebruikers volgens het principe SAAS (software as a service).*
  Gebruikers benaderen IT-toepassingen via internettoepassingen en Cloud-technologie en hebben toegang tot standaard omgevingen die binnen Defensie of door derden worden aangeboden en onderhouden. Voor toepassingen in het inteldomein of bij hoog gerubriceerde omgevingen kan hiervan worden afgeweken.

3.4 Het beoogd landschap van IT-toepassingen (SOLL)

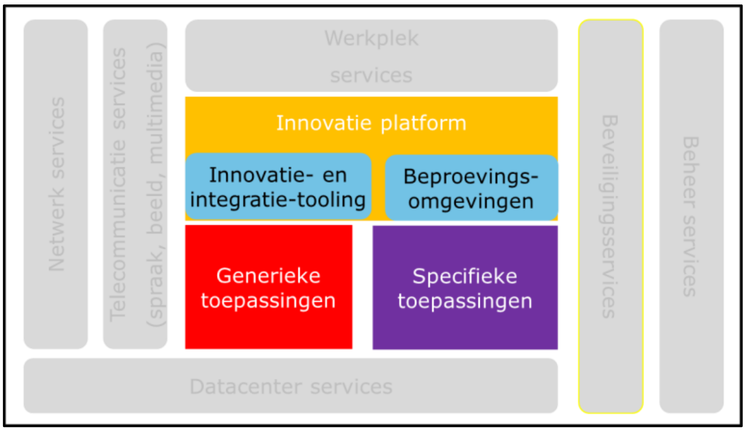
Defensie moet de komende jaren rekening houden met een nog grotere rol van IT, vooral in de Defensie-industrie. Door de enorme toename van sensoren, die onlosmakelijk deel uitmaken van wapensystemen, ontstaan omvangrijke en complexe informatiestromen. Ook systemen voor opleiding, training, medische diagnose en simulatie laten een sterke groei zien van sensoren en grootschalige informatiestromen. Vooral het operationele domein zal steeds afhankelijk worden van IT om snel en betrouwbaar een omgevingsbeeld op te bouwen. De IT-toepassingen leveren meer en meer essentiële informatie op om beslissingen te ondersteunen. De ontwerpprincipes uit paragraaf 3.3 houden rekening met de behoefte om grootschalige informatiestromen te kanaliseren en waar nodig te combineren, zodat medewerkers precies die informatie krijgen die noodzakelijk is voor een specifieke taak of essentiële beslissing.

Om het landschap van IT-toepassingen zodanig in te richten dat wordt voldaan aan de ontwerpprincipes wordt het landschap omgevormd naar een structuur die bestaat uit verschillende domeinen, die zich onafhankelijk kunnen ontwikkelen, maar wel één logisch geheel vormen. Het is essentieel dat de domeinen een eigen ontwikkeling kunnen doormaken om daarmee te borgen dat de verschillende domeinen hun eigen bouwstenen hebben en de bouwstenen veranderbaar zijn, zon-

der het landschap als geheel te destabiliseren. Randvoorwaarde om het landschap van IT-toepassingen in deze domeinen op te delen is de realisatie van de nieuwe technische IT-infrastructuur uit hoofdstuk 4.

3.4.1 *De domeinen van IT-toepassingen in de toekomst*

Onderstaand figuur bevat een impressie van het toekomstige landschap van IT-toepassingen binnen Defensie.



Figuur 9. Vereenvoudigde impressie toekomstig landschap van IT-toepassingen

De inhoud van de verschillende domeinen in het toekomstige landschap van IT-toepassingen is:

1. *Het Gebruikersdomein.* In de toekomst is dit een persoonlijk portaal dat toegang geeft tot de samenwerkingsruimte, tot agendafuncties en taaklijsten. Tevens bevat dit domein de toegang tot de services en systemen die de medewerker nodig heeft, ongeacht het domein waarin deze zich bevinden.
2. *Het Innovatiedomein.* Dit bestaat enerzijds uit *tooling* om IT-toepassingen te integreren en uit specifieke services zoals *Business Proces Management*, *Case Management*, *Business Rule Management* die in staat zijn om transacties en gegevens aan te roepen en ook terug te schrijven in het algemene domein en gedifferentieerde domein. Het innovatiedomein maakt het mogelijk om functionaliteit uit de andere domeinen voor de gebruiker "op maat" te benaderen.

   Daarnaast is dit domein geschikt om gebruik te maken van innovatieve oplossingen die beschikbaar zijn op basis van internettechnologie, cloudoplossingen en gebruik van standaardservices van de markt (*software as a service*).Dit platform is bij uitstek geschikt voor het assembleren van zowel nieuwe IT als huidige IT op een zodanige wijze dat flexibele IT ontstaat voor een flexibele bedrijfsvoering of commandovoering.

   Het innovatiedomein beschikt ook over moderne oplossingen om medewerkers digitaal te laten samenwerken (samenwerkingsruimte). Door de invoering van het innovatiedomein in het landschap van IT-toepassingen kan doelgericht informatie uit meerdere systemen tegelijk worden opgehaald en in de context van een bepaalde taak worden geaggregeerd.

   Het innovatiedomein bevat ook verschillende beproevingsfaciliteiten, *tools* en omgevingen. In dit domein bevinden zich de middelen om nieuwe toepassingen te beproeven of experimenteel in te zetten. Ontwikkelingen in de Defensie-industrie, consumenten-industrie, NATO of Rijksoverheid kunnen op experimentele basis worden gekoppeld met andere toepassingen, worden geëvalueerd en eventueel breder worden ingezet of afgebouwd.

   IT-toepassingendomein: bestaat uit een mix van generieke- en specifieke toepassingen om alle processen en inzetsituaties van Defensie te ondersteunen. In het domein van de IT-

toepassingen vinden we dus nog steeds een mix van generieke (bedrijfsvoerings) IT-toepassingen en van specifieke IT-toepassingen.

3. *Generieke en specifieke IT.* Generieke IT zijn de toepassingen die ook in markt gangbaar zijn. Hieronder zijn ook begrepen de geïntegreerde systemen die gebaseerd zijn op administratieve verwerking van gestandaardiseerde transacties voor Defensiebrede standaard processen zoals ERP. Met deze systemen worden de grootschalige gegevensverzamelingen beheerd met stam- en transactiegegevens.

   De specifieke IT betreffen de toepassingen die bijzonder zijn voor Defensie. Voorbeelden zijn systemen voor commandovoering, opleiding, training, medische ondersteuning, verwerken van sensorinformatie, analysetools, geo-systemen en inlichtingen. Deze systemen zijn niet per definitie uniform voor de gehele krijgsmacht. Een systeem voor commandovoering bij landoptreden kan afwijken van een soortgelijk systeem voor maritiem optreden.

4. *Datadomein.* Dit domein omvat in de toekomst de centrale (*back-end*) voorzieningen om de basisregistraties verder te ontwikkelen en de dataomgevingen geschikt te maken voor nieuwe ontwikkelingen, zoals grootschalige opslag van sensorinformatie, *big data* en datamanagementtooling voor de Intelomgeving. Het datadomein betreft de basisvoorzieningen en de defensiebrede brongegevens. In principe kan iedere IT-toepassing eigen (lokale) dataomgevingen hebben met eigen transactiegegevens en extracten vanuit de basisregistraties. Daarom bevat het datadomein ook lokale voorzieningen waarbij IT-toepassingen eigen data kunnen opslaan en verwerken, ook als netwerkconnectie (tijdelijk) ontbreekt. Lokaal kunnen ook voorzieningen gebruikt worden zoals analyse *tooling* voor lokale data. Deze *tooling* maakt deel uit van het IT-landschap en is een specifieke IT-toepassing.

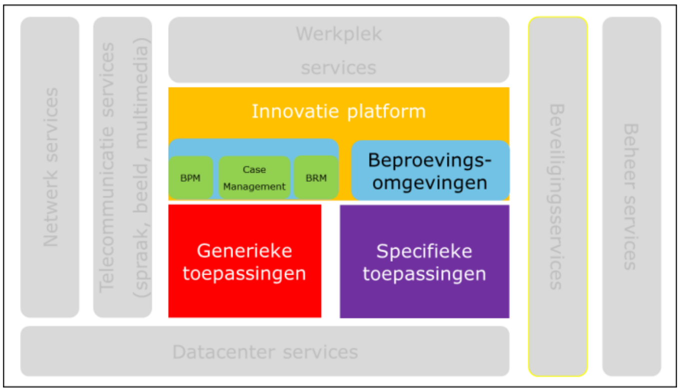
5. *Koppelingen.* Dit zijn koppelingen om flexibel te kunnen samenwerken met partners van Defensie (wereldwijd) en koppelingen om systemen binnen Defensie onderling te laten communiceren (*enterprise service bus*). Tevens bevat de *enterprise service bus* voorzieningen om gebruikers vanuit het gebruikersportaal rechtstreeks toegang te geven tot generieke of specifieke systemen.

6. *Beveiliging.* De ontwikkelingen in de IT hebben voor Defensie grote invloed op veiligheidsaspecten. Samenwerking, wetgeving op het gebied van privacy, vertrouwen van partners stellen steeds hogere eisen aan beveiliging. Tegelijkertijd wordt Defensie meer een "open organisatie" en zijn gebruik van internet, draadloze verbindingen en koppelingen met partners steeds gangbaarder. Ontwikkelingen op het gebied van cyberaanvallen, virussen en *malware* leiden tot een wedloop tussen indringers en beveiligingsmaatregelen hetgeen van Defensie adequate antwoorden vraagt. Het voortdurend herijken van beleid voor informatiebeveiliging en actualiseren van risico's en maatregelen moet gebeuren, rekening houdend met de balans tussen "openheid" en veiligheid.

   Het uitgangspunt achter moderne informatiebeveiliging is dat informatie niet meer alleen beveiligd kan worden door de gangbare mechanismen van afscherming die gericht zijn op de toegang tot gegevens, zoals *firewalls* (bastion principe). Informatie kan in de nabije toekomst, mede door gebruik van internet en de steeds intensievere samenwerking tussen organisaties, alleen nog beveiligd worden door keuzes te maken op het niveau van systeembeveiliging en beveiliging van de gegevens zelf (versleutelen).

3.4.2 *Het nieuwe landschap van IT-toepassingen in relatie tot de nieuwe IT infrastructuur*

Op de nieuwe infrastructuur worden toepassingen geplaatst die vallen binnen het gebruiksdomein, het innovatiedomein en de nieuwe IT-toepassingen die Defensie in gebruik wil nemen. Dit kunnen zowel generieke als specifieke toepassingen zijn. Bovendien zullen de IT-toepassingen die migreerbaar zijn volgens de kaders van de HDBV/CIO en vervolgens de rationalisatiemethodiek eveneens op de nieuwe IT-infra worden geplaatst. Dat betekent dat een deel van de generieke en de specifieke IT om technische of om economische redenen niet zal migreren. Deze niet migreerbare IT-toepassingen blijven zo lang als noodzakelijk, maar wel zo kort als mogelijk op de huidigeIT-infrastructuur draaien. Daarmee zullen zowel de huidigeen nieuwe technologie naast elkaar bestaan. Figuur 10 is een vereenvoudigde en conceptuele weergave van het nieuwe landschap van IT-toepassingen.



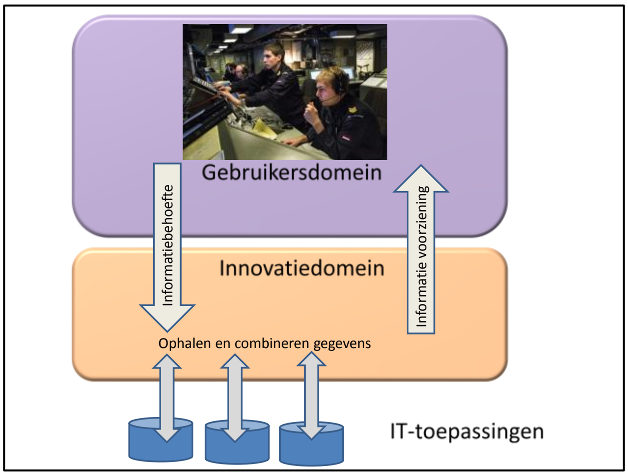
Figuur 10. Vereenvoudigde impressie van de nieuwe IT-infra

3.5 Het innovatiedomein nader toegelicht

3.5.1 *Integratie van generieke en specifieke toepassingen*

Het samenstel van generieke en specifieke IT-toepassingen is niet bijzonder. Vrijwel alle grotere organisatie beschikken over een hybride structuur. Binnen Defensie is deze mix echter in toenemende mate een belemmering omdat steeds meer gegevens gecombineerd gebruikt moeten worden om bijvoorbeeld de commandovoering effectief in te vullen. Medewerkers moeten in verschillende omgevingen gegevens kunnen opvragen en kunnen combineren om bijvoorbeeld een beslissing te nemen in een operationele situatie. Defensie heeft in het bestaande landschap van IT-toepassingen nauwelijks voorzieningen om over de grenzen van toepassingen heen informatie te combineren of meerdere IT-toepassingen gelijktijdig te bevragen of gegevens naar meerdere IT-toepassingen gelijktijdig terug te schrijven. Het innovatiedomein zal daarom vooral voor operationele omstandigheden een *enabler* zijn om informatie naar taak, functie of omstandigheid naar behoefte van de gebruiker (bijvoorbeeld een commandant) te kunnen ontsluiten.

Voor de individuele medewerker moet het niet relevant zijn in welke IT-toepassing gegevens zich bevinden en of dit een generieke of een specifieke toepassing is. De medewerker moet op basis van taak of functie gegevens kunnen aanroepen, zonder gehinderd te worden door technologische grenzen. De *tooling* voor integratie en innovatie in het innovatiedomein beoogt exact deze lacune in het huidige landschap te dichten. De *tooling* is in staat vanuit de optiek van de gebruiker de onderliggende IT-toepassingen logisch te integreren.



Figuur 11. De integratierol van het innovatiedomein

De *tooling* in het innovatiedomein is een schil van services met oplossingen om onderliggende IT-toepassingen te benaderen. In de markt is een zogenaamde *service bus* een beproefd technisch middel om IT-toepassingen te laten communiceren. Het concept *service oriented architecture* is een beproefd middel om met services informatie te verzamelen in een hybride landschap van IT-toepassingen en deze op maat aan gebruikers te presenteren. Ook procesafloop, werkstromen en caseondersteuning die over grenzen van toepassingen heen lopen kunnen in deze laag tot stand worden gebracht (zie Figuur 11).

Het innovatiedomein opent daarmee de technische mogelijkheid om verschillende IT-toepassingen, van verschillende technologieën te integreren en slim te combineren ter ondersteuning van bijvoorbeeld commandovoeringsprocessen, inlichtingenprocessen en ook voor de ondersteunende processen. Het innovatiedomein omzeilt de beperkingen van het huidige systeemlandschap omdat dit een schil van oplossingen bevat die tussen de gebruiker en de IT-toepassingen in staat. Dit domein bevat services om bedrijfsprocessen met elkaar te verbinden en tot een bedrijfsomvattend geheel te combineren (integratie- en *business process* management laag).

3.5.2 Beproeving en experiment

Naast de *tooling* voor integratie worden via het innovatiedomein ook oplossingen beschikbaar gesteld met een zeer korte levensduur of oplossingen met een experimenteel dan wel zeer innovatief karakter waarvan de levensduur nog niet voorspelbaar is. De werkwijze *Concept Development & Experimentation* (CD&E) wordt ondersteund met deze beproevingsomgevingen.

Via de beproevingsomgevingen worden nieuwe toepassingen met Defensie-industrie, markt, NATO of Rijksoverheid beproefd en eventueel experimenteel beschikbaar gesteld. Ook de (specifieke) IT die bij nieuwe wapensystemen of sensoren hoort kan via beproevingsomgevingen experimenteel ter beschikking worden gesteld en na succesvolle beproeving breder worden uitgerold.

3.5.3 Beheerst veranderen en saneren

Na het ontstaan van dit innovatiedomein wordt het ook gemakkelijker om onderdelen van het landschap van IT-toepassingen die verouderd zijn in fasen te moderniseren, zonder dat daarvoor de hele bedrijfsvoering beïnvloed wordt. Er is immers veel minder directe interactie tussen gebruiker en de onderliggende IT-toepassingen.

Bijkomend voordeel is dat het innovatiedomein de mogelijkheden biedt om logica (set van bedrijfsregels) buiten de IT-toepassingen te beheren. Dat betekent dat veranderingen in wetgeving, regelgeving of doctrine niet meer hoeven te leiden tot ingrijpende herbouw van IT-toepassingen, maar

beperkt kunnen blijven tot aanpassing van de bedrijfsregels in een aparte omgeving. Het doorvoeren van veranderingen wordt daarmee eenvoudiger en substantieel goedkoper. Deze manier van werken met bedrijfsregels kan niet voor alle bestaande IT-toepassingen toegepast worden.

Ten slotte vormt het innovatiedomein als geheel een schil om IT-toepassingen en wordt het hele landschap van IT-toepassingen modulair opgebouwd en veranderbaar. Gartner noemt dit innovatiedomein de *systems of innovation*. Hierdoor ontstaat een zogenaamde *pace layered application strategy* die zich kenmerkt door hoge veranderbaarheid en innovatief vermogen.

3.5.4 Nieuwe technologie

In talloze grote organisaties is sprake van een complexe mix van technologieën en een steeds toenemende complexiteit. Marktpartijen spelen daar op in en inmiddels is er technologie voorhanden om de complexiteit vergaand te reduceren. Deze technologieën worden ook door Defensie ingezet om het innovatiedomein te ontwikkelen. Dat zal in kleine kort cyclische en iteratieve stappen gebeuren. Niet alle *business expertise* en geldende afspraken zijn immers op korte termijn in regels te vatten die de *tools* vragen om het landschap te integreren. Daarom wordt dit vooral in nieuwe trajecten toegepast en voortdurend geëvalueerd. Dit onderschrijft de strategie om verouderde IT-toepassingen vooralsnog in stand te houden totdat nieuwe toepassingen beproefd zijn en de bedrijfsvoering adequaat ondersteunen. De gangbare marktconforme technologieën en concepten die de eerdergenoemde *pace layered application strategy* ondersteunen zijn:

- *IT voor Business Proces Management (BPM)*
  Met BPM wordt de bedrijfsvoering continu verbeterd en wordt gestreefd naar optimale ondersteuning van de strategische doelstellingen van een organisatie. IT voor BPM ondersteunt methoden en technieken om de bedrijfsvoering transparant te maken en vervolgens gericht keuzes te maken om optimaal te automatiseren. BPM is primair bedoeld voor de optimalisatie van voorspelbare processen.

- *IT voor Case Management*
  Case Management is voor processen die min of meer onvoorspelbaar zijn. Dit is een methodiek om dynamische vormen van samenwerking te analyseren en te bepalen wanneer actie noodzakelijk is om vervolgens te kunnen bepalen hoe met IT-toepassingen de noodzakelijke actie ondersteund kan worden door de juiste informatie te verstrekken. IT voor Case management is zeer geschikt voor ondersteuning van omgevingen die beslissingsondersteuning vragen. Commandovoering is een voorbeeld.

- *IT voor Business Rule Management* (BRM)
  BRM is software om bedrijfsregels te beheren en vervolgens er voor te zorgen dat IT-toepassingen zich conform deze bedrijfsregels gedragen. Een voorbeeld van bedrijfsregels is wet- en regelgeving.

- *Service Gerichte Architectuur (SGA)*
  SGA staat voor Service Gerichte Architectuur oftewel *Service Oriented Architecture* (SOA). SGA is een softwarearchitectuurmodel met als doel systeemfuncties (services) technisch los te koppelen van de IT-infrastructuur of de programmeertaal. Hierdoor kunnen services voor gebruikers of tussen IT-toepassingen worden ontwikkeld die niet direct worden beïnvloed door de technologie die er onder ligt. Bijkomend voordeel is dat deze service kleinschalig en iteratief ontwikkeld kunnen worden in kort cyclische trajecten. Toepassing van deze technologieën neemt in de markt momenteel een grote vlucht.

- *Beproevingsomgevingen*
  Beproevingsomgevingen bestaan uit een brede en voortdurend veranderende set van *tools* en

IT-toepassingen om nieuwe ontwikkelingen te testen en kleinschalig in te zetten.

BPM, Case Management, BRM, SGA en beproevinsgomgevingen in één samenstel bieden een belangrijk deel van de oplossing om te voorzien in de vereiste flexibiliteit voor de IT van Defensie.

3.6 De ontwikkeling van de Defensiebrede geïntegreerde IT-toepassingen

De grote Defensiebrede IT-toepassingen die in de loop de jaren bedacht en ontwikkeld zijn voor het grootschalig bijhouden en opslaan van data en proceslogica voor geïntegreerde en Defensiebrede processen (*systems of record*), zullen ook in het nieuwe landschap van IT-toepassingen nog langjarig in gebruik blijven. Deze IT-toepassingen zullen echter steeds meer een statisch karakter kennen (lage verandergraad), maar daarentegen wel een betrouwbare en robuuste werking hebben (*designed to last*). Gezien de investeringen die in deze IT-toepassingen zijn gedaan ligt het voor de hand deze IT-toepassingen zo lang als mogelijk (of zo lang als nodig) te blijven uitbaten en de kracht van deze IT-toepassingen te benutten. Deze IT-toepassingen vormen een robuuste basis voor het beheer van uniforme en betrouwbare gegevensbronnen (basisregistraties; eenmalig vastleggen in uniforme bron en meervoudig gebruiken) en voor uniforme processen.

Nieuwe investeringen in deze geïntegreerde grootschalige IT-toepassingen moeten echter kritisch worden afgewogen. Vereiste is wel dat deze toepassingen in de basis volledig zijn uitgerold in de organisatie. De invoering van ERP in M&F dient bijvoorbeeld wel stabiel en volledig te zijn zodat dit systeem nog jaren als bronsysteem in de IT-architectuur effectief benut kan worden.

De generieke *tooling* in het innovatiedomein maakt het technisch mogelijk de kracht van deze geintegreerde IT-toepassingen te blijven benutten, zonder daarvoor nog nieuwe functionaliteit in deze toepassingen te hoeven ontwikkelen. Investering kan beperkt blijven tot het strikt noodzakelijke om het beheer van deze IT-toepassingen te optimaliseren zonder de integratie met andere processen los te laten. Door de nieuwe generieke technologieën die in de markt beschikbaar zijn is uitbreiding van deze IT-toepassingen geen doel op zich meer. Voor alle nieuwe behoeften die binnen Defensie ontstaan op het gebied van deze grootschalige IT-toepassingen wordt per situatie beoordeeld welke technologie het meest geschikt is in termen van kosten, beheerbaarheid, aanpasbaarheid en toekomstvastheid.

3.7 De ontwikkeling van de specifieke IT-toepassingen

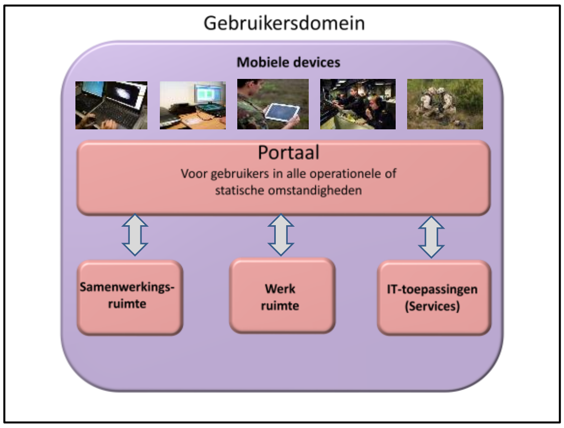
Kenmerkend voor specifieke IT-toepassingen voor het Defensie domein is dat deze toegerust zijn om een bepaalde taak te ondersteunen of een bepaald effect te bereiken. De manier van gebruik ligt echter niet vooraf vast. Deze IT-toepassingen vormen een logische verzameling die bestaat uit bouwstenen (services) met een relatief hoge verandergraad. Daarmee wordt bedoeld dat deze IT-toepassingen zich voortdurend ontwikkelen vanuit de behoefte van bijvoorbeeld commandanten, medewerkers en teams. Als taken, te bereiken effecten, doctrines of regels veranderen dan veranderen de informatiebehoeften vanuit de gebruikers ook en worden de IT-toepassingen of services daarop aangepast.

Essentieel om de veranderbaarheid te borgen is dat IT-toepassingen in dit domein gebaseerd zijn op losse bouwstenen oftewel services die snel te isoleren en te veranderen zijn. Dit domein is vergelijkbaar met een gereedschapskist die voortdurend gevuld wordt met de losse gereedschappen om een bepaalde klus te klaren. De gereedschappen zijn in principe losse elementen, maar ze vormen een samenhangende set, gericht op een bepaalde taak of een te bereiken effect. Commandovoering is een voorbeeld van taken die een set van samenhangende zogenaamde services vragen. Dit betreft services om een omgevingsbeeld op te bouwen, samen te werken met partners (*from sensor to shooter*), eenheden aan te sturen, locaties te bepalen en te interveniëren. Ook het verzamelen van inlichtingen en het analyseren van data vraagt services in dit domein.

De services worden niet gebruikt op basis van een standaard proces, maar op basis van deskundigheid over het te bereiken doel. Soortgelijke situaties om services te gebruiken zien we in medische omgevingen, bij opleiding en training en bij informatie gestuurd optreden. Er zijn dus vele omgevingen binnen Defensie die behoefte hebben aan een flexibele set van services die passen bij taak en doel en eenvoudig kunnen veranderen. Overigens veranderen niet alle IT-toepassingen in dit domein voortdurend, maar de toepassingen zijn wel altijd specifiek voor bepaalde taken of doelen.

3.8 De ontwikkeling van het gebruikersdomein

In de toekomst bestaan de IT-toepassingen in het gebruikersdomein uit een persoonlijk portaal waarin de gebruiker onder alle omstandigheden de toegang vindt naar de omgeving die hij/zij nodig heeft. De gebruiker heeft toegang tot operationele informatie, geo-informatie, omgevingsbeeld, voorziening voor de samenwerking met anderen binnen en buiten Defensie. De behoeften die voortkomt uit de taak van de individuele medewerker is daarbij leidend (zie Figuur 12).



Figuur 12. Vereenvoudigde impressie van het gebruikersdomein

De mate waarin IT-toepassingen aansluiten bij de behoeften van de medewerker is bepalend voor de toegevoegde waarde van IT-toepassingen als geheel. Het gaat daarbij om aspecten als optimaal beslissingen kunnen nemen, kunnen samenwerken, beschikbaarheid van de juiste en betrouwbare omgevingsinformatie op het juiste moment en de juiste plaats, mobiliteit van IT-toepassingen, wereldwijde toegang, samenwerking over de keten heen en kunnen aansluiten bij ontwikkelingen zoals *Internet of Things* en sensortechnologie. Het gebruikersdomein faciliteert de medewerker ongeacht rol of functie om zodoende de productiviteit, operationele effectiviteit en persoonlijke arbeidsvreugde te verbeteren vanuit een portaal waarin de toegang eenvoudig en overzichtelijk geregeld is. In de gewenste situatie is er voor iedere medewerker zowel een koppeling met alle interne data in de IT-toepassingen als een scala aan innovatieve oplossingen voor ondersteunende en operationele taken. Ook samenwerken met gebruik van Social Media behoort tot de mogelijkheden.

De toekomst is dat de medewerker beschikt over een eigen digitale werkruimte en toegang tot samenwerkingsruimtes. Daarnaast heeft hij/zij flexibele apparatuur (*mobile devices*) waarmee eenvoudig toegang wordt verkregen tot de werkruimte en de mogelijkheid bestaat om eigen services toe te voegen.

4. High Level Ontwerp IT-Infrastructuur

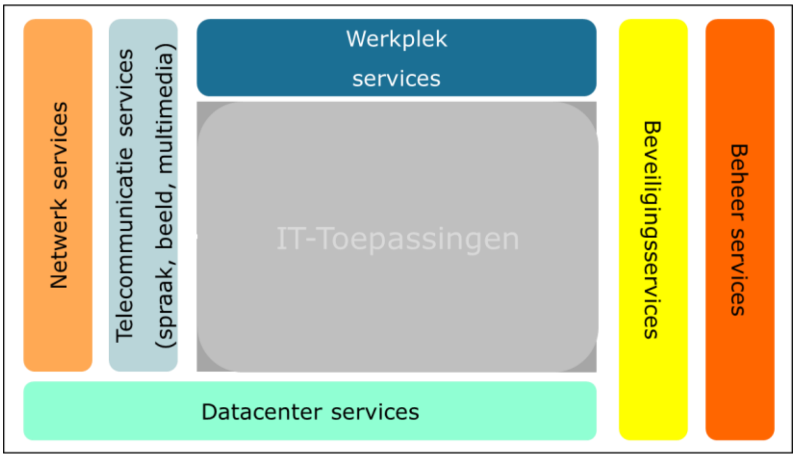
4.1 Inleiding

De IT-infrastructuur is het platform waarop de IT-toepassingen worden aangeboden.

4.2 Structuur huidige IT Infrastructuur

De IT Infrastructuur bestaat op hoofdlijnen uit de volgende onderdelen (zie Figuur 13):

- Netwerk (connectiviteit). Het beschikken over verbindingen om op (LAN) en tussen locaties (WAN) te kunnen communiceren met andere gebruikers en toegang te kunnen krijgen tot *IT-services*. Dit kan binnen een gebouw zijn maar ook naar een operationele commandopost of de militair in het veld. Het gaat zowel om vaste verbindingen als draadloze verbindingen, inclusief satellietcommunicatie.
- Datacenters (applicatiehosting). De voorziening om IT-toepassingen te kunnen *hosten*, gegevens te kunnen verwerken en te kunnen opslaan, zowel statisch centraal als decentraal in ontplooide situatie. Het gaat hier over over de fysieke infrastructuur (datacenternetwerk, opslag, verwerking) en het applicatieplatform (besturing, gegevensbeheer, uitvoering en gegevensuitwissling).
- Telecommunicatie (*communication services*). De voorziening voor het bieden van spraak, tekst en beeldcommunicatie. Het gaat niet alleen om "bellen en gebeld worden" (telefoon, *push-to-talk* radio, e.d.) maar ook om *video conferencing*, semafonie, mobiele telefonie en *call centers*. Telefonie infrastructuren worden ook nog gebruikt voor het koppelen van faciliteiten zoals slagbomen, toegangspoortjes en liften. De spraakfunctionaliteit in het mobiele, uitgestegen en te voet domein (MUT) is grotendeels gebaseerd op basis van diverse militaire radio's.
- (Digitale) Werkplek. De voorziening voor het leveren en ondersteunen van eindgebruikersapparaten (verwerking en besturing) zoals *fat client, thin client, tablet, smartphone*, printer. Het kunnen gebruiken van generieke functionaliteiten (zoals productiviteits- , samenwerkings- en social media tools) en de toegang tot functie specifieke en business specifieke functionaliteiten. Dit is de digitale werkplek.



Figuur 13. Vereenvoudigde weergave van de IT-infrastructuur

Daarnaast zijn er twee aspecten binnen de IT-infrastructuur die betrekking hebben op bovenstaande onderdelen:

- Beheer. Het leveren van een betrouwbare en veilige (geautomatiseerde) IT dienstverlening. Beheer betreft niet alleen het "in de lucht houden van" IT, maar ook het tijdig vernieuwen.
- Beveiliging. Dit is een *enabler* om op een veilige manier digitaal te kunnen werken. Beveiliging

is erop gericht om door het nemen van passende maatregelen de risico's voor de bedrijfsvoering te identificeren, te beheersen en acceptabel te houden. Beveiliging houdt ook in dat voorzien wordt in beveiligingsoplossingen (bijv. crypto, identificatiemiddelen, veilige koppelvlakken) en het implementeren van maatregelen om communicatie mogelijk te maken en te houden. Risico's zoals informatielekken, het verlies van beschikbaarheid en manipulatie van gegevens worden afgedekt.

4.3 Ontwerp principes van de toekomstige IT Infrastructuur

Om de business eisen genoemd in hoofdstuk 2 te realiseren dienen enerzijds de geconstateerde belemmeringen te worden weggenomen en anderzijds de IT infrastructuur te worden gemoderniseerd. Hiertoe zijn ontwerpprincipes gedefinieerd voor de onderdelen van de IT-infrastructuur, die vertaald zijn in ontwikkelrichtingen voor de verschillende onderdelen van de IT infrastructuur.

- <u>SOMUT gebruiksomstandigheden</u>. Deze business eisen omvatten de complete Defensie organisatie: zowel de bedrijfsvoering, de operaties alsook de inlichtingenketen. De IT-Infrastructuur is ondersteunend voor al deze processen. Dit houdt in dat deze structuur ook alle gebruikersomstandigheden moet ondersteunen: statisch, ontplooid, mobiel, uitgestegen en te voet (SOMUT). Hierbij wordt de IT infrastructuur zoveel mogelijk op basis van een gemeenschappelijke architectuur, standaard apparatuur (bv. voor de KMAR te voet) en *tooling* ingericht. Sommige gebruikersomstandigheden vragen echter in bepaalde omstandigheden specifieke oplossingen (bijv. robuuste apparatuur i.v.m. klimatologische omstandigheden, mobiele ad hoc netwerken en decentrale datacenters) en afwijkend beheer.
- <u>Rubriceringscompartimenten</u>. De ontwikkelrichting voor de IT infrastructuur is het realiseren van één geïntegreerde, samenhangende en open - maar beveiligde – infrastructuur, zonder belemmeringen voor de onderlinge communicatie en communicatie met partners. Zolang dit nog niet is gerealiseerd is zijn er nog steeds scheidingen in rubriceringscompartimenten (laag gerubriceerde en hoog gerubriceerde compartimenten, LGI en HGI) nodig binnen een rubriceringsdomein. Defensie kent vier typen rubriceringen, namelijk Departementaal Vertrouwelijk, Stg. Confidentieel, Stg. Geheim en Stg Zeer Geheim. De eerste twee worden ondergebracht in de LGI infrastructuur en de laatste twee in de HGI infrastructuur. In de ontwikkeling wordt de compartimentscheiding van een fysieke scheiding naar logische scheiding en van gescheiden netwerken naar beschermde (gelabelde) informatie. Bij gegevensuitwisseling tussen partners en rubriceringscompartimenten spelen beveiligde koppelvlakken en crypto een belangrijke rol. De mate waarin de scheiding kan plaatsvinden moet per type oplossing beoordeeld worden in een accreditatieproces. STG Confi maakt onderdeel uit van het LGI domein . Externe communicatie en koppelingen met NATO en EU secret vinden alleen plaats via het HGI domein.
- <u>Continue verandering</u>. De technische ontwikkelingen in de IT infrastructuur gaan razendsnel. Defensie wil sneller profiteren van deze nieuwe innovaties. Dat kan alleen door zoveel mogelijk commerciële (commodity) producten te gebruiken en een marktconforme inrichting van de IT. Hiervoor is een modulaire opbouw en standaard koppelvlakken vereist. Dit om sneller nieuwe functionaliteiten te kunnen introduceren en de huidige te vervangen en sneller over te schakelen op modernere apparatuur. Dit vereist een continu innovatieproces om ontwikkelingen te toetsen en beproeven. De veranderende business behoefte leidt tot continue aanpassing van de IT.
- <u>Betaalbare infrastructuur</u>. De IT van de toekomst moet een betaalbaar IT. Dit vereist standaardisatie, harmonisatie en het saneren van de IT-infrastructuur en toepassingen. Het zoveel mogelijk toepassen van standaard commerciële oplossing (*consumerisation*) past ook bij dit uitgangspunt.

Dit zijn de algemene principes voor de IT infrastructuur. In de volgende paragrafen worden de principes steeds voorzien van een afkorting, welke verwijst naar het domein waar het op betrekking heeft. De afkortingen zijn:

ALG : Generieke principes voor de IT Infrastructuur
DC : Datacenter
NW : Netwerk
TC : Telecommunicatie
WA : Werkplek Applicaties
WD : Werkplek Device
BH : Beheer
SE : Beveiliging

De principes zijn gekoppeld aan de doelstelling waar ze het meest op van toepassing zijn. In Bijlage 1 zijn de principes verder uitgewerkt (uitleg, rationale en business eisen). Sommige principes zijn aan verschillende business eisen te koppelen.

Relatie met Business Continuity Management (BCM):

BCM betreft de continuïteit van de bedrijfsvoering voor de (primaire) Defensie processen over de gehele keten. De IT infrastructuur is een belangrijk middel voor het realiseren van continuïteit van de IT toepassingen ten bate van de primaire Defensie taken. In de ontwerp principes is dan ook in belangrijke mate rekening gehouden met de behoeftes qua beschikbaarheid en continuïteit die hier uit voortkomen. In bijlage 2 is een overzicht opgenomen van in welke mate de principes bijdragen aan de behoeften van de business en het continuïteitsbeheer in het bijzonder.

4.3.1 Business thema 1: Business en mens staan centraal, IT sluit aan

- *Functionaliteit.* Gebruikers moeten optimaal worden voorzien van de IT-middelen en functionaliteit om hun taak te kunnen uitvoeren. Qua generieke functionaliteit wil de gebruiker maximaal worden ondersteund met de meest recente productiviteitspakketten, samenwerkingsfunctionaliteiten en moderne multimediale communicatievormen. De generieke functionaliteit voorziet in een gepersonifieerde digitale werkruimte met alle functionaliteiten die bijdragen aan digitaal (samen)werken zoals: persoonlijke toegang tot de digitale wereld, het vinden van mensen en informatie, het kunnen communiceren met anderen, het werken in team- en ketenverband, het delen van kennis en het creëren en vastleggen (archiveren) van informatie.
- *Geïntegreerde oplossingen.* De medewerkers willen geen los staande oplossingen, maar oplossingen die ze geïntegreerd kunnen gebruiken. De generieke voorziening voor de digitale werkplek van de gebruikers is een geïntegreerd platform van productiviteits-, *unified communications*- en social media tools. Waar "spraak" (*voice*) op dit moment een zelfstandige oplossing is zal dit migreren naar multimedia communicatie, waarin verschillende vormen door elkaar gebruikt zullen worden: chat, beelden, video en *voice*. Deze functionaliteiten worden geïntegreerd aangeboden.
- *Devices.* De nieuwe IT moet het werken met een diversiteit aan moderne eindgebruikers apparatuur (ook met niet door Defensie verstrekte middelen) op verschillende locaties mogelijk maken. In het gebruik van verschillende eindgebruikers *devices* kan gemakkelijk worden gewisseld in de loop van de tijd. Draadloze communicatie en mobiele *devices* wordt de standaard voor de eindgebruikers. Hierdoor kan plaatsonafhankelijk gewerkt worden. De standaard manier van het toegang bieden tot toepassingen via de werkplek zal hierdoor *web based* (browser, apps, portal) worden ingevuld. De gebruikersinterface naar de IT-toepassing moeten door de gebruiker aangepast kunnen worden om optimaal toegesneden te zijn voor hun taak. Gebruik van nieuwe *devices* (bijv. *wearables*) moet kunnen worden toegevoegd.

- *Werkplekconcept.* Diverse verschillende los staande oplossingen moeten worden voorkomen. De werkplek moet in verschillende omstandigheden zoveel mogelijk kunnen worden gebruikt en zoveel dezelfde *look-and-feel* hebben. De *business* eisen vragen om een veilig, gestandaardiseerd werkplek concept, dat zowel in operationele als in de statische omgeving kan functioneren en waarbij gebruikers toegang hebben tot zowel hoog gerubriceerde als laag gerubriceerde informatie. Dit gestandaardiseerde concept voorziet in tijd-, plaats-, en *device*-onafhankelijk werken. Innovaties die gebruikers nodig hebben kunnen hier snel en eenvoudig aan toegevoegd worden. Dit vereist flexibiliteit in de apparatuurkeuze[1] en regelmatige actualisatie van de ondersteunde apparaten. Tevens moet het apparaat en de functionaliteit zoveel mogelijk losgekoppeld zijn van elkaar, zodat de applicatie niet belemmerend is voor het toepassen van een moderner *device*. Het kiezen van een juiste standaard voor applicatie ontsluiting (bijv. *browser*) maakt de applicatie onafhankelijk van het apparaat. Er is een sterke innovatie met nieuwe *apps* en *devices* die mensen met elkaar in contact brengt en laat samenwerken. Het volgen hiervan, het toetsen en beproeven (CD&E) in de Defensie context is belangrijk.

Deze business eis leidt tot de volgende ontwerp principes:

- Algemeen:
  ALG.1 Business staat centraal
  De functionele behoefte van de business bepaalt de vorm en inrichting van de IT infrastructuur.

- Voor het Datacenter:
  DC.1 Mix van workloads met verschillende servicelevels
  Het datacenterconcept dient een mix van verschillende werklasten (*workloads*) met verschillende service levels aan te kunnen. Met het datacenterconcept wordt een gedifferentieerd aanbod van services en service niveaus (een *managed diversity*), afhankelijk van de functionele vraag vanuit de business. De hoogste service niveaus voor diensten zijn *never out* en geen dataverlies.

- Voor de Werkplek:
  - ✓ *WA.01 IT functionaliteit wordt vanuit een te personaliseren portal aangeboden aan de gebruiker.*
    Functionaliteit wordt geordend aangeboden via een portaal. Deze portal is door gebruikers te personaliseren en optimaal in te richten op zijn/haar taak.
  - ✓ *WA.02 Presentatie en invoer van gegevens op maat voor gebruik en device*
    Toepassingen dienen *device aware* te zijn ontworpen en daarmee geschikt om op diverse apparaten te draaien (*responsive design*).
  - ✓ *WA.03 Het applicatie portfolio is maximaal onafhankelijk van rubricering en gebruiksomstandigheden*
    Defensie maakt gebruik van een gerationaliseerd applicatie portfolio, wat is gestandaardiseerd over de diverse rubriceringsdomeinen (LGI en HGI) en gebruiksomstandigheden (statisch, ontplooid, mobiel, uitgestegen en te voet).
  - ✓ *WA.04 Het applicatie portfolio is maximaal inzetbaar voor diverse doelgroepen*
    Aan de ontwikkeling en/of aanschaf van toepassingen die Defensie breed kunnen worden

---

1 Op dit moment worden de beveiligingsrisico's bij *any place en any device* werken in combinatie met hoog gerubriceerd te groot geacht om dit mogelijk te maken. De ontwikkelrichting is wel om dit op een zo kort mogelijke termijn wel te realiseren.

ingezet wordt de voorkeur gegeven boven het ontwikkelen/aanschaffen van toepassingen met vergelijkbare of gelijke functionaliteit die slechts voor een deel van Defensie ingezet worden.

- ✓ *WD.01 Any Place, Any Time, Any Device*
  De Defensiemedewerker kan waar dan ook ter wereld, op een willekeurig gekozen moment en op een willekeurig device de taken verrichten die hij moet uitvoeren.
- ✓ *WD.02 Draadloos, tenzij…*
  Medewerkers worden steeds mobieler in de uitvoering van hun taken en moeten daarvoor over informatie en toepassingen kunnen beschikken zonder een fysieke connectie te maken.
- ✓ *WD.03 Devices hebben een digitale identiteit*
  Ieder device is te identificeren bij gebruik van Defensie dienstverlening (traceerbaar).
- ✓ *WD.04 Users hebben een digitale identiteit*
  Iedere gebruiker is te identificeren bij gebruik van Defensie dienstverlening (traceerbaar).
- ✓ *WD.05 Het device portfolio is ingericht op het principe van managed diversity.*
  Medewerkers hebben verschillende werkstijlen. De IT van Defensie ondersteunt deze werkstijlen met een variatie aan *devices* en *end user* platformen. Dit geldt voor allerlei *devices*, waaronder *smart phones* en workstations, en voor een diversiteit aan operating systemen (bijv. Android, Windows, Linux, IOS).

- Voor het Netwerk:
  NW.1 Netwerk ondersteunt draadloze devices
  Het Netwerk ondersteunt bedrade en draadloze *devices* en sensoren. Draadloze Netwerken[2] ondersteunen mobiele *devices* en het plaatsonafhankelijk werken.

- Voor de Telecommunicatie:
  - ✓ *TC.1 Eén geïntegreerde communicatie functionaliteit*
    De communicatie functionaliteit biedt spraak, video, tekstcommunicatie en *presence* voor zowel de statische als ontplooide gebruiksomstandigheid. In het kader van digitaal genetwerkt samenwerken wordt de communicatiefunctionaliteit geïntegreerd met de productiviteits-, samenwerkings- en *social media tools* aangeboden.
  - ✓ *TC.2 Ondersteuning any place en any device*
    De communicatie functionaliteit ondersteunt *any place* en *any device* voor zowel de statische als ontplooide gebruiksomstandigheid. Een gebruiker kan het communicatie-adres (e-mailadres/telefoonnummer) waar functionaliteit wordt aangeboden uit de statische omgeving ook in de ontplooide gebruiksomstandigheid gebruiken en is op dit communicatie-adres overal en in elke situatie bereikbaar.

- Voor het Beheer:
  - ✓ *BH.1 Gebruikers worden ondersteund via selfservice*
    In situaties waarin Defensie niet al automatisch voorziet in IT-benodigdheden, wordt de eindgebruiker in staat gesteld om via een selfserviceportaal[3] zijn (extra) benodigdheden aan te vragen of meldingen te doen. Uiteraard kan hier nog een proces van toestemming voor worden ingericht, maar de essentie is dat de eindgebruiker de trigger geeft via selfservice. Onderdeel van het proces is om de mogelijkheid te hebben om een aantal self service functionaliteiten te kunnen delegeren aan een persoon of functionaris.

---

2 Draadloos LAN is (vooralsnog) alleen in het LGI domein beschikbaar in verband met beveiligingseisen. SATCOM is een draadloze voorziening waar wel HGI overheen wordt gecommuniceerd met goedgekeurde crypto.
3 Voor operationele omstandigheden kunnen andere oplossingen worden gekozen dan *self service*.

- Voor de Beveiliging:
  - ✓ *SE.1 Alle Defensiemedewerkers hebben een persoonsgebonden gebruikersaccount, gebaseerd op de Basisadministratie Digitale Identiteit Defensie*
    Alle Defensiemedewerkers (burgers, militairen en externe inhuur) hebben een persoonsgebonden gebruikersaccount, gebaseerd op de Basisadministratie Digitale Identiteit Defensie. Voorwaarde voor het krijgen van een persoonsgebonden gebruikersaccount is dat de desbetreffende medewerker in de personele basisadministratie van Defensie als actief medewerker staat geregistreerd. De Defensiemedewerker identificeert zich primair met een door Rijksoverheid of Defensie verstrekt identificatiemiddel dat voldoet aan de PKI-overheidsnormen. Na authenticatie krijgt de gebruiker door middel van *Single Sign On* toegang tot alle toepassingen en informatie van desbetreffend beveiligingsniveau én lagere beveiligingsniveaus. De Defensiepas[4] is de komende jaren hét authenticatiemiddel waarmee de Defensiemedewerker zich authentiseert. Dit geldt zowel voor LGI als HGI, voor alle gebruikersomstandigheden (SOMUT). In de toekomst worden wellicht andere identificatie middelen (bijv. de Rijkspas) en authenticatiemethoden mogelijk en goedgekeurd, zoals SIM-kaart op een mobiel.
  - ✓ *SE.5 Autorisaties volgen taakstelling en bedrijfsvoering*
    In de basisregistraties voor Personeel en Organisatie worden mensen verbonden met de taakstelling van Defensie op basis van functie en de organisatie. Dit geschiedt door plaatsing op functies, in onderdelen en toewijzing aan missies en oefeningen. Deze basisregistratie is de basis voor het verstrekken van autorisaties voor de toegang tot data en functionaliteit. Toegang tot data is verder afhankelijk van verschillende parameters zoals de locatie waar de gebruiker werkt, het apparaat waarmee gewerkt wordt en het maximale rubriceringsniveau waarvoor de gebruiker gescreend is..

4.3.2 *Business thema 2: De IT maakt veilig samenwerken in snel wisselende verbanden mogelijk*

Communities of interest. De infrastructuur is in staat om gebruikersdomeinen (*communities of interest*) te realiseren zowel binnen Defensie als met partners. De IT-infrastructuur voorziet daartoe in oplossingen om gezamenlijk in teamverband bijv. tijdens joint, interagency, multinationale en publieke operaties, te kunnen samenwerken. Om (geautoriseerd) toegang te krijgen tot de infrastructuur heeft ieder device en ieder gebruiker een veilige digitale identiteit. Gebruikers van andere organisaties waar Defensie mee samenwerkt worden geautoriseerd op principes van vertrouwensrelaties met 'federated identities'. De informatie en functionaliteit is afgeschermd en kan op basis van verleende toegangsrechten worden verstrekt of gebruikt.

Geconsolideerde infrastructuur. De infrastructuur zal geconsolideerde zijn met zo min mogelijk grenzen in fysieke of logische domeinen. Hier moet gezocht worden naar oplossingen (beveiligingsoplossingen) om dit mogelijk te maken. Grenzen tussen domeinen moeten adequaat beveiligd zijn en het samenwerken met andere domeinen en partijen ondersteunen. Beveiligingsoplossingen zoals koppelvlakken en crypto moeten een *enabler* zijn om veilig communiceren mogelijk te maken.

Open maar veilige infrastructuur. De nieuwe infrastructuur moet veilig zijn. Door het genetwerkt samenwerken is het *bastion*-principe voor beveiliging niet houdbaar. De nieuwe infrastructuur krijgt een open karakter. In specifieke situaties kan nog gekozen worden voor een gesloten oplossing. Dit vraagt naast maatregelen zoals een goede afscherming van de netwerkkoppelingen ook om het beschermen van de data. Snelle crypto op data niveau zijn hiervoor noodzakelijk. Daar-

4 De Defensiepas kan ook geleverd worden door het Rijk in de vorm van Single Service Management.

naast is IT inmiddels dusdanig verweven met de bedrijfsvoering dat de beschikbaarheid van groot belang is. De IT infrastructuur moet beschikbaar zijn, ook wanneer sprake is van gerichte digitale aanvallen op de beschikbaarheid.

Beheer en beveiliging. De IT en de IT-beheerorganisatie voorzien in adequate beveiligingsfuncties- en middelen en nemen adequate maatregelen om de digitale weerbaarheid op peil te houden. Adequaat houdt hierbij in dat de maatregelen proportioneel zijn in relatie tot het risico. De nieuwe infrastructuur biedt een effectief verweer tegen cyber- en andersoortige aanvallen (zoals interceptie) door beveiligingsmaatregelen integraal mee te ontwerpen op basis van risicoanalyse.

Identiteit en toegang. Samenwerken met andere partijen vereist het kunnen delen van informatie en toepassingen. Het waarborgen van de juiste identiteit van de gebruikers en het verlenen van toegang (autorisatie) is kern voor het digitaal samenwerken. Samenwerking vereist een andere kijk op identificatie, authenticatie en autorisatie. Federatief werken met andere partijen vereist IAM (*Identity Access Management*) die dit op een veilige manier mogelijk maakt.

Samenwerkingsfunctionaliteit. Moderne manieren van samenwerken worden ondersteund met functionaliteiten zoals *voice*, video en tekst communicatie (*unified communications*, een digitale samenwerkingsruimte en *social media tools*) waarbij de gebruikers centraal staan.

Deze business eis leidt tot de volgende ontwerp principes:

- Algemeen:
  ALG.2 Federatief samenwerken
  De IT infrastructuur dient federatieve samenwerking te ondersteunen. Defensie heeft NATO Federated Mission Network (FMN) geadopteerd als de standaard voor federatief samenwerken in NATO verband.
- Voor het Datacenter:
  - ✓ *DC.2: Veilig samenwerken in snel wisselende verbanden*
    Tussen verschillende *communities of interest* is informatie-uitwisseling mogelijk. Dat geldt voor alle omgevingen en wordt gefaciliteerd op basis van open standaarden via goedgekeurde koppelingen en gateways. Daartoe liggen datacenters voor verwerking van (hoog) gerubriceerde informatie op een Defensie locatie. HGI en LGI data wordt daarbij fysiek gescheiden verwerkt en opgeslagen. Binnen HGI en LGI wordt compartimentering met behulp van virtualisatie software toegepast. Compartimenten worden door gateways gekoppeld. Het beperkt delen van faciliteiten zoals *housing* is hierbij toegestaan.
  - ✓ *DC.3: Rapid Datacenter deployment*
    Door gebruik te maken van virtualisatie en configuratie management, kan *deployment* van Datacenters tot en met de gebruikte toepassingen voor zowel HGI als LGI in statische en ontplooide situaties grotendeels op basis van hetzelfde model worden ingericht. Repeterende taken op het gebied van *deployment (provisioning)* worden geautomatiseerd en gestandaardiseerd over de verschillende rubriceringen (HGI/LGI) en omstandigheden (SOMUT) heen. Ontplooide Datacenters volgen zoveel mogelijk de standaarden vanuit de statische Datacenters, maar wijken (gemotiveerd) af indien de missie / gebruiksomstandigheid dit vereist.
- Voor de Werkplek:
  - ✓ *WA.05 De werkplek biedt mogelijkheden voor digitale samenwerking in federatieve context*
    Samenwerken in een federatieve context staat centraal in het werkplekconcept en moet eenvoudig mogelijk zijn. Een samenwerkingsomgeving is nodig om informatie te delen en digitaal samen te werken met gebruikers uit andere organisaties (*communities of interest*).

  - ✓ *WD.06 Papierloos werken (kantoor)*
    Defensie streeft naar zoveel mogelijk papierloos te werken, dit om onnodige printen te voorkomen (milieu, *efficiency* en *footprint*).
  - ✓ *WD.07 Defensie optimaliseert continu de weerstand tegen cyber aanvallen*
    Beveiliging is geen eenmalige exercitie. Aanvallers ontwikkelen zich voortdurend, dus moet de verdediging daar continue op aangepast worden *devices*, maar ook *apps*, worden continu geoptimaliseerd om weerstand te bieden tegen deze cyber aanvallen.

- Voor de Telecommunicatie:
  - ✓ *TC.3 HGI heeft eigen middelen voor communicatie*
    Voor communicatie op geheim niveau wordt een communicatie voorziening in HGI opgenomen.
  - ✓ *TC.4 De identiteit van gebruikers van communicatiemiddelen en werkplekken moet beschermd kunnen zijn*
    De identiteit van gebruikers wordt beschermd, vooral in het inzetgebied (OMUT). Het moet mogelijk zijn om gebruikers in deze omstandigheid tijdelijk een afgeschermde digitale identiteit (mee) te geven die na de missie vervalt. Ook moet het mogelijk zijn om nieuwe adressen en gebruikers identiteiten toe te kennen voor personen ter plaatse.

- Voor het Netwerk:
  - ✓ *NW.2 Al het dataverkeer is vercijferd*
    In principe wordt al het dataverkeer vercijferd (initieel op IP niveau door open VPN of crypto en uiteindelijk op applicatie/dataniveau).
  - ✓ *NW.3 Het netwerk brengt overal IP*
    De standaard van het netwerk is gebaseerd op IP. Voor het netwerk (en dus de toepassingen die hier op werken) is de nieuwe standaard IPv6. De overgangsfase is gebaseerd op *dual-stack* (IPv4 en IPv6).

- Voor het Beheer:
  - ✓ *BH.2 Beheer is voor de LGI- en de HGI-ketens ingericht volgens dezelfde processen*
    Beide *delivery en support* ketens dienen hetzelfde *proces-framework* te gebruiken en dezelfde kwaliteitsattributen in de SLA's te ondersteunen om de gedeelde klant te faciliteren. De ketens zijn waar mogelijk, geïntegreerd. De gebruiksomstandigheden bepalen hoe "zwaar" de processen zijn ingevuld.

- Voor de Beveiliging:
  - ✓ *SE.2 Defensie vertrouwt het identiteitsbeheer van vertrouwde partners waarmee Defensie federatief samenwerkt.*
    Defensie registreert identiteiten van Defensiemedewerkers inclusief alle attributen die relevant zijn voor het verstrekken van logische en fysieke toegang. Voor het beheer van identiteiten van externe gebruikers vertrouwt Defensie op het identiteitsbeheer van de externe, vertrouwde partij.
  - ✓ *SE.3 Handelingen die worden uitgevoerd op platforms en toepassingen kunnen naar een natuurlijke persoon worden herleid*
    Alle (vanuit beveiligingsoogpunt relevante) handelingen die worden uitgevoerd op de IT infrastructuur en in de IT toepassingen zijn herleidbaar naar de uitvoerder als natuurlijk persoon. Er mag geen toegang worden gegeven tot IT toepassingen op het Netwerk als de gebruiker niet is geauthentiseerd. Relevante handelingen van de gebruiker worden geregistreerd, waarbij een eenduidige koppeling te leggen tussen een gebruikt account en een natuurlijk persoon. Indien er functionele accounts worden gebruikt, moet wel duidelijk zijn

wie (gebruiker/natuurlijke persoon) op welk moment welke functie heeft vervuld.

In de basisregistraties voor Personeel en Organisatie worden mensen verbonden met de taakstelling van Defensie. Dit geschiedt door plaatsing op functies, in onderdelen en toewijzing aan missies en oefeningen.

- ✓ *SE.4 Fysieke en logische toegangsbeveiliging zijn geïntegreerd*
  Fysieke toegangsbeveiliging en de logische toegangsbeveiliging worden geïntegreerd op basis van gemeenschappelijke elementen Hierbij kan worden gedacht aan het toegangsmiddel voor de Defensiemedewerker (de Defensiepas), services voor identity management en aan attributen behorende bij de digitale identiteit, zoals de organisatierol, centraal opgeslagen policies en toegangsregels.
- ✓ *SE.6 IT infrastructuur is ontworpen op basis van de uitgangspunten Security by Design, Defence in Depth en Diversity in Defence*
  De IT infrastructuur krijgt een open karakter. Dreigingen kunnen zich overal in de IT infrastructuur manifesteren. Dit wijzigende dreigingsbeeld vraagt om gelaagde beveiligingsfuncties in alle delen van die IT infrastructuur. Beveiliging moet worden ingebouwd in plaats van (later) worden toegepast. Dit geldt ook voor de beveiligingsproducten die in de IT infrastructuur worden ingezet.

4.3.3 Business thema 3: IT is betrouwbaar en beschikbaar

Hoog beschikbaar. De nieuwe IT-infrastructuur is hoog beschikbaar. De geboden services zijn essentieel voor de gebruikers om hun werk te kunnen doen. Gebruikers en bedrijfsprocessen verwachten dat deze niet uitvalt en dat 24x7 uur kan worden doorgewerkt. De IT-infrastructuur en dienstverleningsniveaus moeten aansluiten bij deze verwachtingen. Gebruikers moeten in alle omstandigheden door kunnen werken, ook in de ontplooide situatie. Indien zich onverhoopt problemen voordoen met de IT-infrastructuur moet het mogelijk zijn om de dienstverlening geleidelijk te verminderen (*graceful degradation*) en abrupte uitval moet worden voorkomen.

Never out en gedistribueerd. Cruciale onderdelen[5] van de IT infrastructuur zijn ontworpen op een *never out* principe. Rekening wordt gehouden met het autonoom kunnen doorwerken in operationele omstandigheden indien de verbinding niet beschikbaar is. Een gedistribueerde implementatie (centraal en decentraal) bij operationeel optreden is derhalve mogelijk. De IT-infrastructuur in ontplooide omstandigheden is dusdanig in geregeld dat de lokale *footprint* zo klein mogelijk is. Dit geldt ook voor het beheer van de lokale IT.

Beheer. Beheer is gericht op het waarborgen van de correcte werking van de IT-infrastructuur en het gecontroleerd kunnen aanpassen daarvan. De correcte werking houdt in dat de afgesproken serviceniveaus inclusief de beveiliging worden gerealiseerd. De beheerprocessen zijn niet alleen gericht op het draaiende houden van de IT maar ook op het flexibel wijzigen van de infra en deze snel te kunnen aanpassen (*life cycle management*). De betrouwbaarheid en beschikbaarheid van de IT moet worden bewaakt. Beheer is zoveel mogelijk proactief ingeregeld waarbij de beheertaken zoveel als mogelijk zijn geautomatiseerd.

Deze business eis leidt tot de volgende ontwerp principes:

- Voor het Datacenter:
  DC.4: Scale-out toepassingen hebben voorkeur
  Scale-out toepassingen, die geautomatiseerd resources alloceren of de-alloceren (*cloud aware*)

5 De business moet dit nog nader specificeren om te kunnen bepalen welke toepassingen en delen van de infrastructuur hiervoor *never out* moeten worden ingericht.

hebben de voorkeur boven *scale-up* toepassingen, waarbij infrastructuur resources handmatig worden toegewezen. *Scale-out* toepassingen vereisen minimaal drie locaties voor optimale werking.

- Voor de Beveiliging:
  - ✓ *SE.7 De beveiligingsfuncties stellen het beveiligen van de data centraal*
    Het belangrijkste deel van de IT infrastructuur is de data. Deze moet beschikbaar en toegankelijk zijn wanneer deze nodig is en niet toegankelijk zijn wanneer dit niet wenselijk is. De risicoanalyse en het ontwerp van de IT nemen de data als uitgangspunt. Te nemen beveiligingsfuncties binnen de IT infrastructuur zijn primair ingericht vanuit de gedachte dat de toegang tot data geautoriseerd wordt in plaats van toegang tot de applicatie of infrastructuur. Het is de data zelf die vercijferd wordt in plaats van de verwerkende IT infrastructuur en als een applicatie niet werkt moet de data nog wel toegankelijk zijn.
  - ✓ *SE.8 Integrale geautomatiseerde en meetbare (Cyber) Situational Awareness over alle informatiedomeinen en IT infrastructuur heen*
    Een geslaagde aanval kan niet worden altijd voorkomen, wel kan de schade van een aanval beperkt worden. Dit vraagt om goed ingerichte (Cyber) *Situational Awareness* zodat verdachte signalen zo snel mogelijk opgepikt worden. Dit vraagt erom dat het zo veel mogelijk geautomatiseerd, detecterend en reactief vermogen (handelend inclusief herstellend vermogen) met een integraal beeld over de staat van de gehele IT infrastructuur.
  - ✓ *SE.9 In de IT-infrastructuur worden voor de kritische beveiligingsfuncties producten met bekende en goedgekeurde kwaliteit ingezet*
    De Rijksoverheid inclusief Defensie en ook EU- en NATO stellen specifieke eisen aan de kwaliteit en betrouwbaarheid van beveiligingstechnologie. In de Nederlandse regelgeving staat dat transport van gerubriceerde informatie over niet vertrouwde netwerken met ministerieel goedgekeurde cryptografische middelen dient te worden uitgevoerd. Dit vraagt om certificatie van beveiligingstechnologie en producten die *secure by design* zijn. Hetzelfde geldt voor communicatie in missieverband, waar ook goedgekeurde producten moeten worden toegepast.

- Voor het Netwerk:
  - ✓ *NW.4 Adhoc Netwerk concept voor MUT omstandigheden*
    In de MUT gebruiksomstandigheden kiest Defensie voor een Netwerkconcept gebaseerd op ad-hoc networking dat verschillende communicatiemiddelen (Satcom; 3G;4G; WiFi; militaire radio etc.) ondersteunt. Hiermee is het mogelijk om een maximale beschikbaarheid en bereikbaarheid in MUT omstandigheden te realiseren.
  - ✓ *NW.5 Netwerk ondersteunt last IT standing bij bijzondere omstandigheden*
    Het netwerk biedt een hoge beschikbaarheid door redundantie van verbindingen. Daarnaast is hoge beschikbaarheid mogelijk doordat het Defensie netwerk onafhankelijk kan werken van de openbare infrastructuren bij bijzondere omstandigheden. Indien een gedeelte van het netwerk wegvalt, kunnen overige locaties blijven doorwerken. Dit is vooral belangrijk voor het ontplooide gedeelte van het WAN.

- Voor de Telecommunicatie:
  - ✓ *TC.5 Specifieke communicatiefunctionaliteit bij MUT omstandigheid*
    In de MUT omstandigheid worden voor de gebruiksomstandigheden specifieke hierop afgestemde functionaliteiten vereist. Spraak is ook hier een *last resort* en heeft een hoge beschikbaarheid. Dit vraagt om specifiek hierop afgestemde communicatievoorzieningen.

- Voor het beheer:

- ✓ *BH.3 Lifecycle management is ingericht voor elke IT-dienst*
  De IT dienstverlener richt integraal *life cycle management* in voor de IT-diensten/services die zij levert. Deze diensten worden actueel en *state-of-the-art* gehouden en aangepast, vervangen of beëindigd naar de behoefte van de gebruikersorganisatie en de beschikbare middelen. Innovatie en instandhouding worden door een kleine kwalitatief excellente groep mensen uitgevoerd. Er is geen organisatorisch onderscheid naar technische *skills*. DevOps (*Development and IT Operations*) voor infrastructuur is een trendbreuk in werkwijze, organisatie, mensen en sturing.
- ✓ *BH.4 Lokaal beheer in OMUT omstandigheden*
  Het wegvallen van (voldoende) connectiviteit noodzaakt maatregelen voor autonoom functioneren, *graceful degradation*, lokaal beheer en eventueel herstel van centraal beheer.

4.3.4 Business thema 4: Met IT is Defensie 'wereldwijd connected'

<u>Netwerk</u>. Netwerkvoorzieningen zijn overal nodig waar Defensie opereert om de functionaliteiten en informatie te kunnen benaderen en te communiceren. Dit betekent een flexibel concept om over een willekeurige netwerkinfrastructuur veilige verbindingen te kunnen realiseren.

<u>Koppelingen</u>. Robuuste koppelingen en voldoende bandbreedte voor centraal-decentrale verbindingen zijn hiervoor noodzakelijk. Het netwerk moet zowel voorzien in de koppeling van de verschillende gebruikersplatformen als in de koppelingen voor het verzamelen van data (bijv. sensoren).

<u>Capaciteit en bandbreedte</u>. Het toenemend gebruik van informatiesystemen en invoering van nieuwe sensoren leidt tot een sterk toenemend volume van informatie dat verzameld en uitgewisseld moet worden over het LAN en WAN. In combinatie met het verkleinen van de *footprint* in het operatie gebied door via *reachback* de missie te ondersteunen vanuit Nederland betekent dit een aanzienlijke groei in behoefte aan bandbreedte in het WAN.

<u>Zwartnet</u>. Missies worden in coalitieverband uitgevoerd. In plaats van altijd een eigen WAN uit te rollen, wordt van elkaars netwerken gebruik gemaakt vanuit het *Protected Core Network* (PCN) concept. *Network Enabled Capabilities* (NEC) en *Network Information Infrastructure* (NII) zijn leidend voor de architectuur van het netwerk. De NII is het 'Defensie internet' dat samenwerken tussen geautoriseerde gebruikers en toegang tot juiste informatie altijd en overal mogelijk maakt. Deze business eisen vragen om een open netwerk concept ('zwartnet') dat vanuit verschillende netwerken (NAFIN, NATO, RIJK en internet) veilig toegang geeft tot het Defensie Netwerk en dat samenwerken tussen de verschillende doelgroepen mogelijk maakt.

<u>Draadloos</u>. Veel *devices* (*any device*) kunnen niet meer bedraad worden aangeschaft en Defensie zal dus moeten inzetten op oplossingen om veilig draadloos te kunnen communiceren. Door naast de bedrade voorziening ook te voorzien in draadloze voorzieningen wordt verder ingespeeld op in tijd-, plaats-, en *device* onafhankelijk werken.

<u>Logische gescheiden netwerken</u>. De betrouwbaarheids- en beschikbaarheidseis gaat zover dat delen van de netwerkinfrastructuur blijven werken, ook als de commerciële netwerkproviders en energieproviders niet meer kunnen leveren. De vertrouwelijkheid van het netwerkverkeer moet kunnen worden garanderen door voor verschillende samenwerkingsverbanden en rubriceringsniveaus hiervoor logisch gescheiden netwerken te kunnen realiseren.

<u>Operationele netwerken</u>. Ook in de mobiele, uitgestegen en te voet (MUT) situatie wordt voorzien in ondersteunende IT-functionaliteiten en communicatie. De individuele soldaat in het veld wordt

netwerkfunctionaliteit geboden. Mobiele *adhoc networking*[6] is hiervoor vereist. Moderne radio's blijven een belangrijk communicatiemiddel voor het operationele domein. Deze moeten blijven werken als alle andere communicatiemiddelen zijn uitgevallen.

Flexibiliteit. Het moet mogelijk zijn om snel kunnen wisselen van netwerkprovider of te wisselen tussen een commerciële *provider* en het gebruik van de Defensie eigen netwerkinfrastructuur (statisch en ontplooid). Dit geldt ook voor *providers* voor mobiele telefonie. Het hebben van eigen mobiele netwerken vereist hiervoor aangepaste oplossing voor de netwerkinfrastructuur om te kunnen *roamen* met mobiele netwerkproviders en bijvoorbeeld ook de SIM-kaart voor het mobiele device.

Deze business eis leidt tot de volgende ontwerp principes:

- Algemeen:
  - ✓ *ALG.3 De infrastructuur ondersteunt verschillende gebruiksomstandigheden*
    De infrastructuur ondersteunt alle gebruiksomstandigheden (SOMUT). De statische en ontplooide gebruiksomstandigheden worden gelijkvormig ingericht (niet alleen op basis van gemeenschappelijke IT standaarden maar ook op gemeenschappelijk gebruikte technische componenten. Mobiel, uitgestegen en te-voet worden eveneens gelijkvormig ingericht. De infrastructuur dient de gehele informatieketen te ondersteunen van statisch tot en met te voet (gesloten C2 keten conform NII). De systemen zijn wereldwijd inzetbaar en moeten daarom geschikt zijn voor een diversiteit van klimatologische omstandigheden.
- Voor het Datacenter:
  - ✓ *DC.5: Autonoom werken in het veld*
    Defensie voorziet voor ontplooide gebruiksomstandigheden in autonome Datacenters voor *compounds,* commandoposten, schepen en andere locaties waar operationele inzet van IT benodigd is. Kritische[7] toepassingen draaien lokaal op deze autonome Datacenters, welke redundant zijn uitgevoerd. Opslag, analyse en verwerking van grote hoeveelheden gestructureerde en ongestructureerde data (*big data*) van diverse sensoren in het veld moeten dicht bij de bron mogelijk zijn. Autonomie vereist decentrale IT, gedistribueerde toepassingen en (beperkt) lokaal beheer, op het niveau van *compounds*, commandoposten, schepen en voertuigen.
- Voor de Werkplek:
  - ✓ *WD.08 Always connected, tenzij…*
    Uitgangspunt voor de statische gebruiksomstandigheden is dat het *device* altijd *connected* is. Voor mobiele en ontplooide omstandigheden is de configuratie van het *device* optimaal ingericht om ook bij het verbreken van de connectie de taak van de gebruiker te blijven ondersteunen.
- Voor het Netwerk:
  - ✓ *NW.6 Netwerk voor veilige communicatie op elke locatie en voor elk niveau van rubricering en met elke partner buiten Defensie*
    De permanente en snelle informatiebehoefte van de Defensie medewerkers vraagt om een hoge beschikbaarheid van het netwerk. Het drager netwerk (Zwartnet) biedt de mogelijkheid om de netwerkinfrastructuur zoveel mogelijk te delen voor verschillende rubriceringsdomeinen Het Zwartnet strekt zich uit over alle SOMUT gebruikersomstandigheden en

---

6 Waar mogelijk wordt gebruik gemaakt van commercieel verkrijgbare netwerkfunctionaliteit; bijvoorbeeld de operationele KMAR medewerker bij grenscontrole.

7 Welke applicaties missie-kritisch zijn bepaalt de business, in dit geval de CDS en de OPCO's. De missie-kritische applicaties die worden meegenomen op missie kunnen zowel "met" als "zonder *reachback"* werken.

maakt het gebruik van een groot scala aan transmissiemiddelen mogelijk, inclusief internet. Het delen van transportcapaciteit met NATO partners is mogelijk via gestandaardiseerde koppelvlakken (conform de NATO PCN standaard).

- ✓ *NW.7 Authenticatie en autorisatie voor elk device*
  Toegang tot het Netwerk is alleen mogelijk na vaststelling dat het een geautoriseerde gebruiker en een geautoriseerd device betreft (*Network Access Control*).
- ✓ *NW.8 Het IP-Netwerk is "transmissie agnostisch"*
  Het IP-Netwerk is "transmissie agnostisch" d.w.z. dat het elk transmissie middel (satelliet, straalverbindingen, huurlijnen, militaire radio, wifi, 4G en internet) moet ondersteunen. In expeditionaire omstandigheden is de beschikbaarheid van transmissiemiddelen afhankelijk van de situatie. Een transmissie agnostisch systeem biedt mogelijkheid om vrijwel in alle situaties het meest effectieve middel te gebruiken.

- Voor de Telecommunicatie:
  - ✓ *TC.6 Waar nodig gebruik maken van eigen mobiele netwerken*
    Indien de omstandigheden er om vragen maakt Defensie gebruik van eigen mobiele netwerken. Daarnaast maakt Defensie indien mogelijk gebruik van commerciële netwerken, waarbij het verkeer zo efficiënt mogelijk wordt getransporteerd (bijv. op basis van *Least Cost Routing*). Om dit zo flexibel mogelijk te kunnen doen en *roaming* met verschillende netwerken mogelijk maken, gebruikt Defensie eigen SIM kaarten.

4.3.5 Business thema 5: IT kan grote hoeveelheden informatie verwerken, opslaan en analyseren

<u>Datacenters</u>. De business eisen vragen om minimaal een hoog beschikbaar data center concept, waarbij vooral de schaalbaarheid van capaciteit en inrichting van continuïteit opnieuw worden opgezet. Deze dienen over voldoende verwerkings- en opslagcapaciteit te beschikken. Dit betekent dat ook robuuste centrale verwerkingscapaciteit (Datacenter) aanwezig is.

<u>Integraal datacenter concept</u>. Het nieuwe datacenter concept is een integraal concept, dat rekening houdt met de eisen aan flexibiliteit, beschikbaarheid en betrouwbaarheid. Het datacenterconcept is een integraal concept, omdat operaties, bedrijfsvoering en inlichtingen niet meer los van elkaar staan. Het geïntegreerde concept reikt ook over de grenzen van centraal en decentraal en van hoog en laag gerubriceerd. Door uit te gaan van een integraal concept wordt snelle ontplooibaarheid mogelijk bij het voorbereiden van een missie. Dit concept kent omwille van eisen van autonomie zowel centrale als decentrale datacenters. Eveneens is op basis van een risicoanalyse scheiding tussen laag en hoog gerubriceerde informatieverwerking en opslag.

<u>Capaciteit</u>. De gevraagde datacenter capaciteit zal toenemen. Zowel voor de opslag van data als de verwerking ervan. De grote hoeveelheid aan informatie die wordt verzameld door het toenemende aantal sensoren, moet in decentrale en centrale Datacenters verwerkt kunnen worden om te leiden tot een goede *situational awareness* en beslissingsondersteunende informatie. Om in de verwerking, opslag en analyse van zeer grote hoeveelheden data te voorzien, wordt in het nieuwe datacenterconcept een *high performance module* voor big data voorzien. De IT-infrastructuur zal voorzien in digitale archief functionaliteit, om grote hoeveelheden data voor langere tijd (digitaal duurzaam) te bewaren conform de wet- en regelgeving. Er moet efficiënt worden omgegaan met het opslaan met informatie. Waar mogelijk wordt data niet gedupliceerd en data die van een bron wordt betrokken dient niet nog eens dubbel te worden opgeslagen.

Deze business eis leidt tot de volgende ontwerp principes:

- Voor het Datacenter:
  - ✓ *DC.6: Opslag, analyse en verwerking van grote hoeveelheden gestructureerde en onge-*

structureerde data (big data) van diverse sensoren, zowel in statische omgevingen als in het veld, moet mogelijk zijn
Zowel in statische omgevingen als in het veld wordt veel data verzameld. Denk aan grote sensoren, zoals bij verkenningsvluchten, UAV's, bewakingscamera's of EOV in het veld. Deze informatie moet verwerkt kunnen worden. Veel data wordt verzameld op locaties waar niet altijd grote netwerkbandbreedte beschikbaar is. In die gevallen moet opslag, analyse en verwerking van grote hoeveelheden gestructureerde en ongestructureerde data (*big data*) dicht bij de bron mogelijk zijn.

4.3.6 *Business thema 6: De IT is eenvoudig en snel aanpasbaar*

Modulair. Dit betekent dat de IT-infrastructuur flexibel en gemakkelijk aanpasbaar is. Dit geldt voor alle IT-services. Door een modulaire opbouw wordt hier een invulling aan gegeven. Hierdoor kunnen verouderde componenten en functionaliteiten snel worden vervangen door nieuwe exemplaren. Missies moeten snel kunnen worden ontplooid. Dit vereist ook een flexibel concept om de benodigde IT-infrastructuur hiervoor gereed te stellen.

Cloud-principe. De digitale werkomgeving is zodanig ingericht, dat functionaliteiten snel kunnen worden toegevoegd. Deze functionaliteiten kunnen ook van andere partijen (bijv. internet, commercieel, Rijk en NATO) komen en moeten gemakkelijk geïntegreerd kunnen worden. Hiervoor wordt het cloud-principe toegepast. Defensie maakt optimaal gebruik van het internet waar de beveiliging en continuïteit van de dienstverlening dit toelaat. Hiervoor dienen conform de *National Institute of Standards and Technology* (NIST) de bijbehorende rollen te worden geïmplementeerd om deze nieuwe infrastructuur op de juiste manier te kunnen uitrusten. Als intermediair tussen de *demand* enerzijds en de *supply* (*cloudproviders* en *cloudcarriers*) is in de NIST de *cloudbrokerrol* gedefinieerd, met als taak het samenstellen en dynamisch aanpassen en aanbieden van *cloudservices* van (verschillende) *cloudproviders*.

Software defined. Om invulling te geven aan de eis van flexibiliteit verschuift het beheer van componenten naar services. Het in toenemende mate toepassen van *software defined services* maakt dit mogelijk. De trend gevolgd worden dat robuustheid (*resilience*) steeds meer in de applicatie (*software*) wordt geregeld, in plaats van in de platformservers in het datacenter.

End-to-end. Beheer gaat over de gehele keten (van statisch tot mobiel) en is *end-to-end* ingeregeld. Het beheer is dusdanig ingeregeld dat de benodigde lokale capaciteit in het operationeel domein zo klein mogelijk is.

Deze business eis leidt tot de volgende ontwerp principes:

- Voor het Datacenter:
  - ✓ *DC.7: Defensie private cloud[8] en groei naar hybride cloud[9]*
    De datacenters van Defensie vormen een *private cloud* waarbij de interne- en externe communicatie is gebaseerd op open standaarden. De infrastructuur wordt ingericht met het idee dat deze als *private cloud* wordt gebruikt en gekoppeld met externe omgevingen. In toenemende mate wordt gebruik gemaakt van functionaliteiten uit andere *clouds*, waardoor effectief sprake is van een *hybride cloud*. De *cloud* wordt ingericht conform de NIST principes en standaarden, waaronder de rol van *cloudbroker*.
  - ✓ *DC.8: Modulaire Datacenters*
    De datacenters van de toekomst, zowel de statische als ontplooide en mobiele, zijn modu-

8 *Private cloud* is een geautomatiseerd geheel, wat voldoet aan de kenmerken van NIST en bevindt zich op een Defensie locatie.
9 *Hybride cloud* is een samenstel van eigen *cloud* diensten (*private cloud*) met diensten van anderen.

lair opgebouwd. Modules worden eenvoudig toegevoegd of verwijderd. Dat vertaalt zich in:

- De infrastructuur in de datacenters moet flexibel schaalbaar zijn op basis van eenvoudig aan en af te koppelen modules. Iedere module levert een bepaalde functionaliteit, capaciteit en *performance* (bijv. rekenkracht en/of opslag capaciteit).
- Gebruik voor ontplooide datacenters gestandaardiseerde modules (bouwblokken) met volledige datacenter functionaliteit die automatisch uitgerold kunnen worden, inclusief besturingssystemen en toepassingen.
- Daar waar netwerkverbindingen niet toereikend zijn om alle data centraal op te slaan en te verwerken, moet de opslag en verwerking van data dicht bij de bron (decentraal of in het veld) mogelijk zijn. Dit vereist gestandaardiseerde bouwblokken voor decentrale data verwerking, zowel in Nederland als in het veld.
- De datacenters worden voorzien van efficiënte en milieu vriendelijke stroom en koelings faciliteiten, zodat de schaalbaarheid van deze voorzieningen geen beperkende factor is voor groei.

- Voor de Werkplek:

  ✓ *WA.06 Gebruik cloud aware applications*

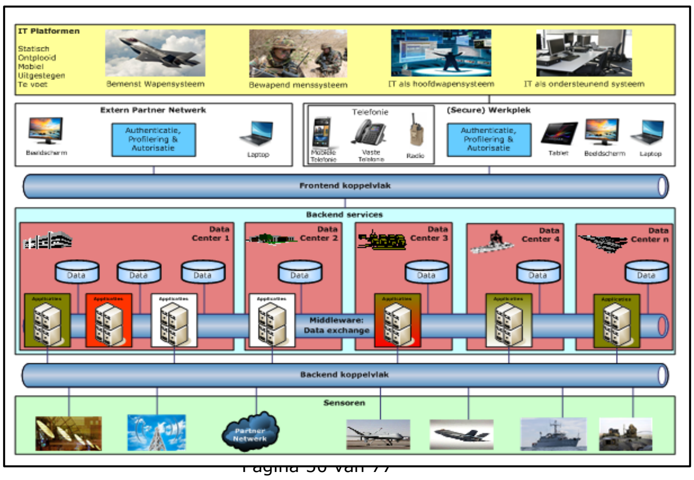
  Moderne toepassingen vereisen minder resources om dezelfde beschikbaarheid te borgen. De applicatie gebruikt *cloud* voorzieningen in de datacenters, is *stateless* geprogrammeerd en draait op een moderne *browser*.
- Voor het Beheer:

  ✓ *BH.5 Geautomatiseerd beheer met moderne tooling*

  Alle beheerfunctionaliteiten worden zo veel mogelijk geautomatiseerd en centraal (redundant) gepositioneerd in de centrale beheeromgeving op alle (aangesloten) Defensie netwerken met verschillende rubriceringsniveaus. De beheerfunctionaliteiten worden enkelvoudig neergezet in de centrale omgeving, hetgeen dubbele (beheer-)functionaliteiten voorkomt. Dit concept betekent onder andere één logisch configuratiedatabase en één centrale tijdbron. In de gehele IT-keten (van switch tot server tot desktop) is end-to-end inzicht om uiteindelijk IT dienstverlening te kunnen leveren tegen een afgesproken *service level*. De IT ondersteunt snelle missieplanning en *deployment* zodat missies nagenoeg in *zero time* kunnen worden gestart. De beschikbaarheid van de IT vormt hierin geen belemmering maar een *enabler*.

4.4 Beoogde ontwikkelrichting voor de IT infrastructuur

Tegen de IT-infrastructuur kan op verschillende manieren worden aangekeken. Vanuit gebruikersperspectief zijn er bepaalde functionaliteiten via de digitale werkplek en is er een "onzichtbaar" deel: de *backend*. Vanuit de levernacier en beheer van IT is er de volgende indeling functionaliteiten (IT services): Netwerk (connectiviteit), Datacenters (applicatiehosting), Telecommunicatie (*communications*), (Digitale) werkplek, Beheer en Beveiliging. Figuur 14 bevat een overzicht van de samenhang in de IT-infrastructuur.



Figuur 14. Samenhang IT-infrastructuur

Een korte omschrijving van de elementen uit bovenstaand figuur is:

- IT-platformen. De relatie tussen gebruikers en het IT-platform kan worden opgedeeld in vier typen: een bemenst wapensysteem (bijv. F-35), een bewapend menssysteem (de moderne soldaat), IT als hoofdwapensysteem (bijv. SIGINT) en IT als ondersteunend systeem (bijv. ERP en Word).
- Sensoren. Naast gebruikers zijn er ook koppelingen voor het verkrijgen van data (bijv. voor sensoren). Een sensor kent diverse verschijningsvormen: schotels en antennes voor interceptie, een netwerk van een partner, drones, vliegtuigen voor beelden en video's, schepen voor sonardata en soldaten in theater voor fysieke waarnemingen.
- *Backend services*. Vanuit de *backend* services wordt daadwerkelijk de functionaliteit geboden aan de gebruikers. Deze verzorgen ook de informatieverwerking en dataopslag.
- (*Secure*) werkplek en telefonie. De werkplek of de telefoon is het zichtbare *device* en *interface* van de gebruiker tot de door de *backend* geleverde functionaliteiten en informatie
- Koppelvlakken. Via koppelvlakken wordt de communicatie en het datatransport verzorgd naar de *backend* services. Ook partners van Defensie kunnen hier toegang toe krijgen en kunnen gekoppeld worden. Uiteraard gebeurt dit op een veilige wijze.

De volgende paragrafen bevatten voor ieder van deze services de ontwikkelrichting.

4.4.1 Datacenters

Datacenters voorzien de opslag en verwerking van gegevens voor toepassingen van (applicatiehosting). Hieronder zijn de kenmerkende aspecten van de toekomstige Datacenters van Defensie weergegeven.

Geïntegreerd. De Defensie Datacenters van de "IT van de toekomst" vormen een geïntegreerd concept. Deze Datacenters zijn schaalbaar en flexibel en kunnen diverse werklasten aan om de gewenste functionaliteit aan de gebruikers te bieden. Redundantie is op een efficiënte wijze ingeregeld om de gewenste betrouwbaarheid en beschikbaarheid te bieden. Het Datacenter concept ondersteund een gedistribueerd concept (centraal en decentraal) en faciliteert zowel hoog als laag gerubriceerde informatieverwerking en opslag (HGI en LGI). De Datacenters zijn hoog beschikbaar en kunnen de *never out* eis ondersteunen voor de cruciale informatiesystemen. De nieuwe Datacenters kennen een modulaire opbouw en zijn gebaseerd op moderne principes zoals cloud, *software-defined* en virtualisatie.

Cloud. Defensie gaat niet alleen toepassingen gebruiken die in de eigen infrastructuur draaien. De toepassingen en data kunnen ook elders vandaan komen (Rijk, NATO, Internet). Om in deze mix de juiste keuzes te maken en deze hybride situatie te beheersen dient een zogenaamde *cloudbroker* rol (conform NIST) ingevuld te worden.

Flexibel en high performance. De Defensie Datacenters zijn snel in te richten (*zero day deployment*) bij het voorbereiden van een missie. De Datacenters voorzien in *high performance* voor o.a. *big data* analyse.

Beschikbaarheid. Bij de inrichting van de Datacenters is er een wisselwerking met de toepassingen. Moderne toepassingen zijn in staat om zelf voor een hoge beschikbaarheid te zorgen. De meeste bestaande toepassingen kunnen dit niet en daarom zal de Datacenter infrastructuur deze moeten regelen. De ontwikkelrichting is hoog beschikbare toepassingen. Voor de migratie van bestaande toepassingen zal (interim) ook hoog beschikbare Datacenter infrastructuur nodig zijn.

Schaalbaarheid. Een zelfde ontwikkelrichting geldt voor de schaalbaarheid. Deze kan geregeld

worden in moderne applicatie (*scale out* toepassingen) of in de infrastructuur (*scale up* infrastructuur). Ook hiervoor geldt dat de ontwikkelrichting de *scale out* toepassingen zijn. Voor de migratie van bestaande toepassingen zal (interim) ook *scale up* datacenter infrastructuur nodig zijn.

Deze nieuwe koers zal niet (direct) kunnen leiden tot vervanging of omzetten van alle toepassingen in *cloud aware* toepassingen. De eis voor nieuwe toepassingen en aan te passen toepassingen is dat deze *cloud aware* zijn en bij voorkeur *scale out*. Dit zal per applicatie op tactische *life cycle* momenten bekeken moeten worden. De datacenters zullen daarom beide vormen dienen te ondersteunen: *scale out* toepassingen en *scale up* voorzieningen in de infrastructuur. De toekom is nadrukkelijk om schaalbaarheid en beschikbaarheid door de nieuwe toepassingen te laten regelen in plaats van in de infrastructuur.

4.4.2 *Werkplek*

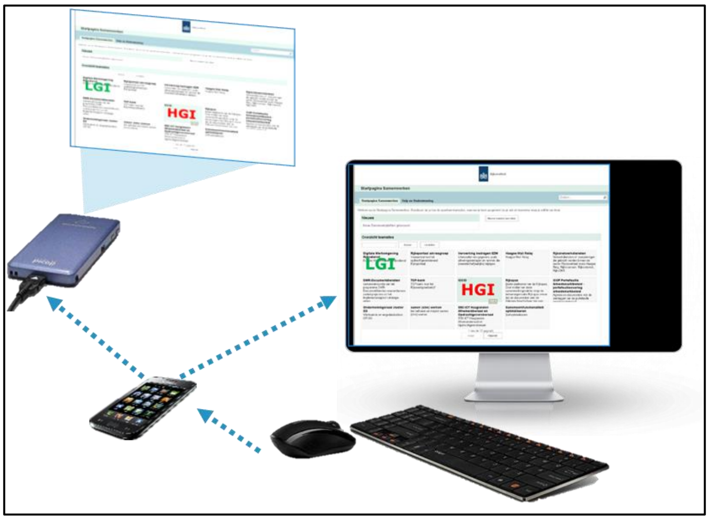
De digitale werkplek is het device waarmee de gebruiker toegang krijgt tot alle functionaliteiten en informatie om zijn werk te kunnen doen. Deze werkplek voorziet in generieke functionaliteiten en geeft toegang tot specifieke functionaliteiten. Hieronder zijn de kenmerkende aspecten van de toekomstige digitale werkplek van Defensie weergegeven.

<u>Variëteit in (mobiele) *devices*</u>. De digitale werkplek vormt de kern van de gebruikersinterface en zal de komende jaren steeds meer verschijningsvormen kennen, zowel in - toenemende mate in - de vorm van mobiele persoongebonden *devices*, als in - sterk afnemende mate - de vaste werkplek. De geleverde of ondersteunde *devices* zijn er in verschillende varianten die optimaal zijn afgestemd op de gebruikersomstandigheden.

<u>*Bring your own device*</u>. Gebruikers brengen zelf apparatuur mee en verwachten dat ze die in de Defensie context overal en altijd kunnen gebruiken (*any place, any time and any device*), zowel in laag als hoog gerubriceerde omgevingen.

<u>Enkelvoudige werkplek voor verschillende domeinen</u>. Er is in de toekomst sprake van een enkelvoudige werkplek, voor die gebruikers die in verschillende omgevingen (hoog en laag gerubriceerd) werken.

<u>Centralisatie functionaliteit</u>. Flexibiliteit vereist een verdere centralisatie van de werkplekfunctionaliteit naar een op web toegang gebaseerde (browser, apps) technologie. De functionaliteit wordt geboden vanuit de veilige Defensie omgeving en door andere cloudproviders (Rijk, NATO, Internet). Ook moeten koppelingen met partners en tussen omgeving als onderdeel hiervan veilig worden ingevuld. Figuur 15 bevat een schematische weergave van de toekomstige werkplek.



Figuur 15. Multi level secure device (de werkplek van de toekomst)

Portalen. De functionaliteit is beschikbaar achter persoonlijke portalen en is via de browser op te halen door het aanbieden van functionaliteit in een *Defensie App Store*. Delen van toepassingen (*apps*) kunnen op deze manier flexibel naar een *device* worden gehaald en zelfstandig worden gebruikt.

Any place, any device, any time. De ontwikkelrichting is *any place, any device, any time*. In hoeverre functionaliteiten van andere providers kunnen worden afgenomen, ieder apparaat daadwerkelijk zonder meer gebruikt mogen worden en iedere functionaliteit op iedere locatie benaderd mag worden, is afhankelijk van de uitkomst van een risicoanalyse die rekening houd met de gevoeligheid van de informatie en de gebruikersomstandigheden (zie ook principes voor beveiliging).

4.4.3 *Netwerk*

Het Netwerk voorziet in de betrouwbare verbindingen tussen gebruikers, sensoren en datacenters en maakt communiceren met andere gebruikers en met andere netwerken mogelijk. De volgende opsomming bevat de kenmerkende aspecten van het toekomstige netwerk van Defensie.

Groei capaciteit. Het toenemend gebruik van informatiesystemen en invoering van nieuwe sensoren leidt tot veel meer informatie die verzameld en uitgewisseld moet worden over het LAN en WAN. In combinatie met het verkleinen van de *footprint* in het operatie gebied door met *reachback* de missie te ondersteunen vanuit Nederland betekent dit een aanzienlijke groei in behoefte aan bandbreedte in het WAN.

Any place. Het netwerk moet zo flexibel zijn dat overal communicatie kan worden geboden. Missies worden doorgaans in coalitieverband uitgevoerd. Dat betekend dat in plaats van overal een eigen netwerk uit te rollen, van elkaars netwerken gebruik gemaakt zal moeten worden.

End-to-end connectiviteit. Het concept voor het netwerk is een geïntegreerd concept. Dit omdat *end-to-end* verbindingen moeten kunnen worden gerealiseerd. Dit gaat over de grenzen heen van de eigen infrastructuur en aanvullend wordt gebruik gemaakt van de publieke infrastructuur en de infrastructuur van partner-netwerken.

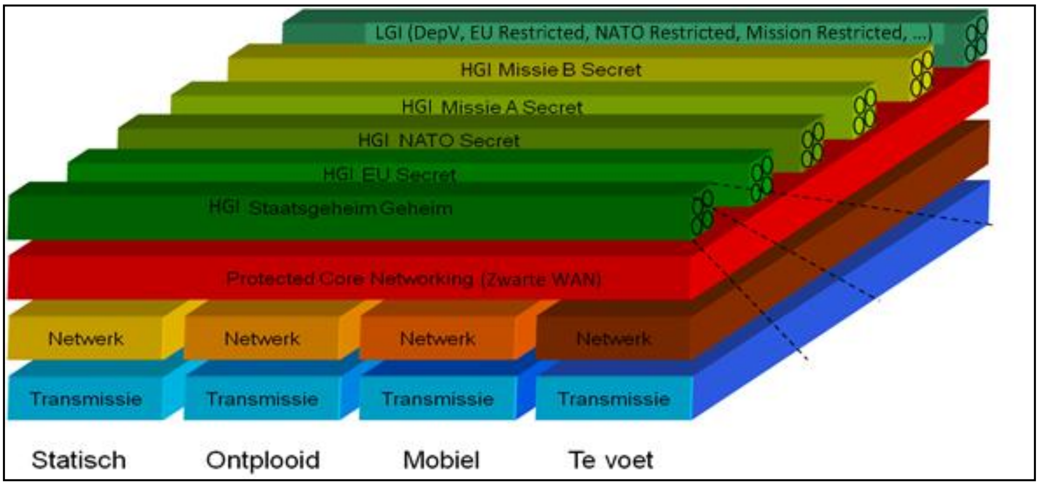
‘*Zwartnet’.* De business eisen vragen om een open netwerk concept (‘zwartnet’), dat vanuit verschillende netwerken (NAFIN, NATO, RIJK, Internet, etc) veilig toegang geeft tot het Defensie netwerk en samenwerken tussen de verschillende doelgroepen mogelijk maakt. Defensie beschikt over een IP gebaseerd ‘zwart WAN’ bestaande uit een *protected core* voor het statische en ontplooide domein, aangevuld met een mobiel *adhoc networking* voor het MUT domein. In het statische domein wordt de *protected core* zoveel mogelijk ingevuld met het breedbandige eigen netwerk (NAFIN) aangevuld met internet en *service provider* diensten waar het te beschermen belang dit toelaat. Binnen het ontplooide domein wordt dit ingevuld door gebruik te maken van internet en service provider diensten. Anderzijds wordt dit ingevuld door uitbreiding van eigen transmissiecapaciteit zoals 4G (LTE), straalverbindingen en satelliet capaciteit. De *deployed protected core* wordt gekoppeld met de *statische protected core*. In ontplooide omstandigheden moet rekening worden gehouden met de mogelijkheid dat de WAN capaciteit tijdelijk volledig kan wegvallen, bijvoorbeeld door netwerkstoringen of de noodzaak tot radiostilte.

Het ‘zwartnet’ dient als generieke drager waarover de informatiedomeinen LGI, HGI en internet gerealiseerd kunnen worden, en ook, wanneer nodig, informatiedomeinen van derden. Het gebruikte sleutelmateriaal in crypto‘s scheidt daarbij de informatiedomeinen. Hierbij wordt gebruik gemaakt van goedgekeurd sleutelmateriaal.

LAN. Het lokale netwerk is het deel waar de gebruiker in de meeste gevallen aan koppelt. Dit is in

toenemende mate een draadloze oplossing. Het LAN in het statische en ontplooide domein bestaat uit een gedeelde infrastructuur voor het leveren van Defensie complex brede connectiviteit. Deze infrastructuur levert toegang tot het LGI informatiedomein en verlengt de *protected core* (zie Figuur 16) tot het gewenste gebouw en ruimte.

Wireless. Door naast de bedrade aansluiting ook te voorzien in draadloze verbindingen wordt verder ingespeeld op in tijd-, plaats-, en device-onafhankelijk werken. Veel devices (any device) kunnen zelfs niet meer bedraad worden aangeschaft en Defensie zal dus moeten inzetten op oplossingen om veilig draadloos te kunnen communiceren. Draadloze verbindingen zullen gerealiseerd worden door gebruik te maken van onder meer WiFi en mogelijk LTE (4G). Door gebruik te maken van Distributed Antenna Systems (DAS) wordt het bereik van de draadloze netwerken in gebouwen en op schepen vergroot.



Figuur 16. Netwerk PCN concept in verschillende gebruikersomstandigheden

Scheiding van netwerken. Scheiding van netwerken wordt zoveel mogelijk op logisch niveau geregeld. Voor omgevingen met een hoog te beschermen belang is dit nog niet altijd toegestaan. Hier zijn nog *dedicated* gescheiden netwerken beschikbaar. Dit deel van het netwerk (LAN) wordt zoveel mogelijk beperkt tot een bepaald gebouw / ruimte of deel van de compound / schip / commandopost.

Betrouwbaarheid netwerkkoppelingen. De mate van betrouwbaarheid van de netwerkvoorziening sluit daarbij aan op de operationele behoefte (het te beschermen belang [TBB]) van de gebruikers en de sensoren. De betrouwbaarheid en redundantie in de bekabeling en de netwerkruimten is navenant ingericht. De activiteiten van de Luchtverkeersleiding of KMAR grensbewaking zullen bijvoorbeeld vanwege de plaatsgebondenheid een hogere IT beschikbaarheid van de werkplek en de toegang tot het datacenter vereisen dan een medewerker die *any place* kan werken. Cruciale locaties worden waar mogelijk via de Defensie eigen netwerk infrastructuur ontsloten.

4.4.4 Telecommunicatie

Telecommunicatie functionaliteit is nodig om het samenwerken mogelijk te maken. Waar "spraak" (*voice*) op dit moment de standaard invulling is, zal dit migreren naar multimedia communicatie. Er is een sterke innovatie met nieuwe *apps* die mensen met elkaar in contact brengt en laat samenwerken. Voor het operationele domein blijft de "radio" een belangrijk communicatiemiddel en moet het blijven doen als andere communicatiemiddelen zijn uitgevallen.

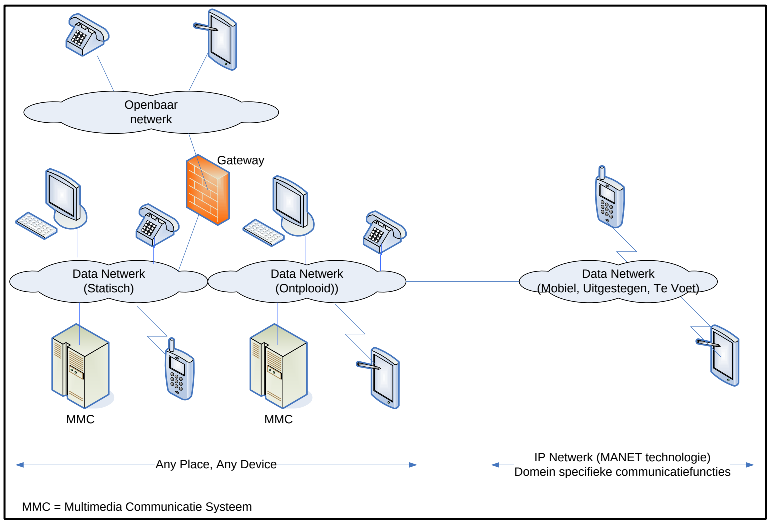
End to end communicatie. Het doel is een *end-to-end* communicatiesysteem voor heel Defensie

(ook voor hoog gerubriceerd en operationeel gebruik) dat gekoppeld is c.q. kan worden gekoppeld met externe partijen. Dit geïntegreerde multimedia communicatie systeem voor statisch en ontplooide gebruiksomstandigheden ondersteunt spraak, video, tekstcommunicatie (*chat*) en *presence*. Een gebruiker kan hierbij vanuit één *end user device* (werkplek, mobiele *device*) veilig communiceren, informatie uitwisselen en samenwerken met alle andere gebruikers in de keten. Deze keten omvat ook partners die bijvoorbeeld via het internet zijn gekoppeld.

Twee oplossingsrichtingen. Voor het toekomstige communicatiesysteem is een tweedeling voorzien, namelijk een geïntegreerd systeem voor zowel de statische als ontplooide omgeving en een systeem voor de mobiele, uitgestegen en te voet (MUT) gebruiksomstandigheden. Deze aparte omgeving voor MUT is buiten Nederland nodig in verband met operationele overwegingen en de technische beperkingen die specifieke gebruiksomstandigheden met zich meebrengen (geen afhankelijkheid van publieke / openbare infrastructuren).

Federatief samenwerken. De communicatievoorziening biedt een veilig koppelvlak met externe communicatiesystemen. Dit koppelvlak voldoet aan de FMN (*Federated Mission Network*) eisen alsmede gangbare interface protocollen voor multimedia communicatie. Koppelingen zijn mogelijk met het internet (vanuit LGI domein), met het publieke telefonie netwerk, met NATO partners en tussen het Nederlandse LGI en HGI netwerk.

Any Device. Het geïntegreerde multimedia communicatiesysteem kan op diverse type randapparatuur gebruikt worden. De ondersteunde apparaten zijn onder meer vaste telefoons, specifieke VTC sets, PC's en mobiele apparaten. De mogelijkheden van het apparaat bepalen daarbij de beschikbare functionaliteiten. De functionaliteit is identiek voor statisch of ontplooid gebruik en gebruikers zullen over de mogelijkheid beschikken om in beide omgevingen dezelfde apparatuur en adressen (telefoonnummer/ SIP adres) te gebruiken (zie Figuur 17).



Figuur 17. Multi Media Communicatie (MMC) in relatie tot de verschillende communicatie systemen

De geïntegreerde multimedia communicatievoorziening voor statisch en ontplooid is zowel voor LGI als voor HGI inzetbaar. Kanttekening is dat voor HGI, vooralsnog, geen bruikbaar en geaccrediteerd draadloos netwerk beschikbaar is en dus geen mobiele apparatuur toegepast kan worden. Het is wel mogelijk om met behulp van speciale toestellen, voorzien van een voor *Secret* geaccrediteerde crypto, over *Unclass* en *DepV* netwerken geheim te communiceren.

4.4.5 Beveiliging

Beveiliging heeft op de gehele IT Infrastructuur betrekking. Beveiliging moet in de nieuwe IT Infra-

structuur een *enabler* zijn om genetwerkt samenwerken optimaal mogelijk te maken. De aard van de taken van de krijgsmacht maakt dat voor bepaalde toepassingen hoge eisen aan de beveiliging gesteld worden. De vertrouwelijkheid, integriteit, authenticiteit, beschikbaarheid en onweerlegbaarheid van informatie moet geborgd zijn. Informatie moet voor de juiste persoon op het juiste moment en op de juiste plaats beschikbaar zijn. In een context waarbij sprake is van diverse niveaus van dreiging is dit een uitdaging.

<u>Centrale monitoring.</u> Een *Security Operation Center* (SOC) is essentieel om de veiligheid van de infrastructuur te bewaken en adequaat te reageren op bedreigingen en zwakheden. Bedreigingen kunnen overal in de IT-infrastructuur zich voordoen. Zwakheden (bijv. lekken) kunnen zich in alle componenten zich openbaren. De organisatie moet continu alert zijn om bedreigingen en zwakheden te ontdekken en hier tijdig op reageren.

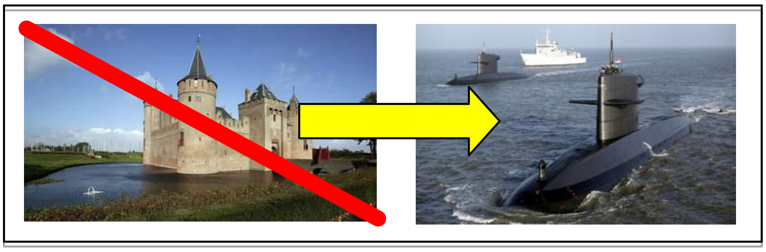
<u>Identiteit als service.</u> *Identity en Access Management* (IAM) is een belangrijke service in de IT Infrastructuur om geautoriseerd toegang te bieden tot informatie en functionaliteit. Deze IAM moet goed worden ingeregeld in een federatieve context waarin wordt samengewerkt en informatie wordt gedeeld met andere partijen. Het is niet automatisch zo dat partijen die door Defensie worden vertrouwd ook elkaar per definitie (moeten) vertrouwen. Naast de identiteit is er ook nog autorisatie (access control). De toegangsrechten worden dusdanig ingeperkt dat men niet overal toegang toe heeft en dat 'doorlussen' wordt voorkomen. Deze rechten worden binnen de digitale samenwerkingsruimtes ingeperkt.

<u>Koppelvlakken en Crypto.</u> In het kader van beveiliging zijn beschikbaarheid van veilige goedgekeurde koppelvlakken en van goedgekeurde snelle encryptiemiddelen noodzakelijk om de vereiste samenwerking wereldwijd te kunnen realiseren. Veilige koppelingen faciliteren de samenwerking tussen verschillende gebruikersgroepen binnen en tussen verschillende security domeinen. Door encryptie wordt de integriteit en de vertrouwelijkheid van de data beschermd. Deze zullen op hoge snelheid (*high speed*) moeten kunnen vercijferen en ontcijferen. Naast netwerkvercijfering wordt datavercijfering belangrijk.

<u>Maatregelen van grens naar data.</u> Op dit moment is de technische beveiliging van nagenoeg alle Defensie systemen ingericht vanuit een *bastion* gedachte. De filosofie dat systemen fysiek afgeschermd moeten zijn van de buitenwereld, interne medewerkers volledig te vertrouwen zijn en dat daarom nauwelijks dreiging uitgaat richting de systemen in het bastion. Vijanden staan in deze gedachte immers buiten de poort en deze kunnen van veraf gedetecteerd worden.

Er is echter sprake van een steeds toenemende behoefte en zichtbare meerwaarde van digitaal samenwerken en werken in federaties. In de IT-infrastructuur vraagt dit om koppelingen tussen systemen, waaronder ook koppelingen met systemen waar mogelijk minder vertrouwen in is. Dit kan minder vertrouwen in de eigenaar van het systeem betekenen, maar ook in de staat van de beveiligingsmaatregelen (bijv. de staat van beheer) in het andere systeem.

De *bastion* gedachte past niet meer, omdat voor het realiseren van koppelingen de valbrug van het bastion dient te worden neergelaten. Er dringt zich meer een vergelijking met het principe van *submarine warfare* op, omdat in een ontsloten netwerk van systemen de aanvaller zich overal kan bevinden en overal kan opduiken (Figuur 18).



Figuur 18. Van Bastion naar risico management

Genetwerkt samenwerken. De eigenschap van de IT-infrastructuur die de meeste invloed zal hebben op beveiliging is de vergaande connectiviteit met andere (niet onder eigen beheer staande) systemen en netwerken. Alle beveiligingsprocessen (van preventie tot herstel) moeten met het uitgangspunt van volledig genetwerkt systeem worden ingericht. Dit brengt aanvullende complexiteit met zich mee en vraagt om methodes zoals onder architectuur / integraal ontwerpen van beveiligingsfuncties en werken op basis van risicomanagement.

Ontwikkeling van de beveiliging. De beveiliging van de toekomstige geïntegreerde IT-infrastructuur is gebaseerd op de volgende uitgangspunten:

- federatief werken met diverse organisaties mogelijk is in verschillende verschijningsvormen, zoals gebruik maken van elkaars netwerk en systemen, delen van informatie door middel van samenwerkingsruimten of faciliteren van organisaties;
- alle informatie voorzien is van een beveiligingslabel;
- beveiligingsmaatregelen voor vertrouwelijkheid gericht zijn op het beschermen van (toegang tot) de data;
- voldoende robuust weerstand geboden kan worden tegen gerichte aanvallen tegen de beschikbaarheid;
- simultaan gewerkt kan worden in verschillende – ook niet onder eigen beheer staande IT omgevingen;
- de infrastructuur toegankelijk is voor alle gebruikers, waarbij niet iedereen een passende Verklaring van Geen Bezwaar heeft;
- de informatie geautoriseerd wordt verstrekt aan vertrouwde gebruikers op basis van een gevalideerde sterke digitale identiteit.

4.4.6 Beheer

Ook beheer heeft net als beveiliging een dimensie die betrekking heeft op de gehele IT-infrastructuur. De betrouwbaarheid en beschikbaarheid moet worden gemonitord en bewaakt. De geboden services en bijbehorende serviceniveaus zijn essentieel voor de gebruikers om hun werk te kunnen doen. Adequaat moeten worden gehandeld (in toenemende mate geautomatiseerd en proactief) om de IT services op het vereiste niveau ter beschikking te stellen aan de gebruikers. De gebruikers eisen toenemende flexibiliteit met betrekking tot de IT-diensten die zij nodig achten voor de ondersteuning van hun werkzaamheden. Dit houdt in dat naast het werkend houden van de infrastructuur ook het snel kunnen bieden van nieuwe of aangepaste diensten afgestemd op de veranderende vraag vanuit de business steeds belangrijker wordt.

Dienstverlening moet aansluiten op de business behoefte. De ontwikkelrichting voor het beheer is het doorvoeren van modern *IT Service Management* (ITSM). Hier ligt de nadruk op het blijvend laten aansluiten van de *IT services* en dienstverleningsniveaus op de behoeften van de business. Dit vereist het flexibeler kunnen aanpassen van de infrastructuur en een snelle *service delivery*. Dit vertaalt zich in verder gaande automatisering van het beheer, het bieden van *self service*, moderne beheer *tooling* (o.a. voor *orchestration*) en een nauwere integratie tussen de ontwikkeling en

het beheer (*DevOps: Development and IT Operations*). Deze trendbreuk ligt niet alleen op het gebied van technologie maar vooral ook op het gebied van mensen en processen. Ook de skills van de beheerders en de beheercapaciteit (centraal en decentraal) moeten in overeenstemming zijn met hetgeen vanuit de business wordt vereist.

Geautomatiseerd beheer. Geautomatiseerd beheer in een moderne *cloud* omgeving vraagt om een significant ander soort IT specialist. De vaardigheden moeten gericht zijn op de integrale keten van gebruikte IT-infrastructuur en integrale procesverantwoordelijken in plaats van individuele proces-managers. Concreet betekent dat de IT specialisten ook verantwoordelijk zijn voor de processen en dat de nadruk ligt op het bieden van integrale beschikbaarheid en continue verandering.

5. Integrale verander- en migratieprincipes

Het systeemlandschap wordt in een aantal stappen gesaneerd, gemoderniseerd en ontwikkeld. De bestaande IT-toepassingen blijven waar noodzakelijk gedurende deze verandering in gebruik om de processen binnen Defensie te ondersteunen (tot en met de operationele inzet).

Onderstaand overzicht bevat de principes voor een beheerste modernisering en ontwikkeling van het systeemlandschap, rekening houdend met de continuïteit van de IT-toepassingen voor Defensie.

5.1 Continuïteit

1. Naast de huidige IT-infrastructuur wordt een nieuwe infrastructuur ingericht. De huidige structuur blijft nog intact zolang nodig. De HDBV/CIO bewaakt dat deze periode zo kort als mogelijk is. Op de huidige structuur zijn - voor zover noodzakelijk - huidige IT-toepassingen beschikbaar. De nieuwe infrastructuur kenmerkt zich door een opzet als groeikern, die meegroeit met de behoeften van de krijgsmacht.
2. Er is beslist geen sprake van een *big bang* scenario waarbij alle huidige IT-toepassingen onverkort migreren naar nieuwe IT-infrastructuur. De migratie van de bestaande IT-toepassingen naar een nieuwe technische omgeving is complex en kan risico's opleveren voor de continuïteit. Er wordt derhalve geleidelijk gemigreerd en toepassingen worden afgebouwd.
3. IT-toepassingen migreren alleen naar de nieuwe IT-infrastructuur op basis van een assessment om de continuïteit te waarborgen. De nieuwe IT-infrastructuur is de basis voor nieuwe, moderne, modulair opgebouwde IT-toepassingen op basis van moderne technologieën en marktstandaarden (zoals SAAS, Cloud en internettechnologie). IT-toepassingen op het bestaande systeemlandschap worden eerst beoordeeld (assessment) voordat migratie naar de nieuwe omgeving wordt gepland (zie tevens hoofdstuk migratieprincipes). Hiermee wordt voorkomen dat de continuïteit van IT-toepassingen degenereert door een migratie naar een platform waarvoor de toepassing technisch niet geschikt is.

5.2 Voorbereiding en kaderstelling voor de migratie

1. De HDBV/CIO stelt kaders om de processen te vereenvoudigen en daarmee ook het bestand aan bestaande IT-applicaties ingrijpend te saneren of samen te voegen. De rationalisatie vindt plaats langs de lijn van verlagen van de TCO (Total Cost of Ownership), reductie complexiteit en verhogen beheersbaarheid en tot slot een kortere *time to market* van aanpassingen en nieuwe applicaties (apps).
2. Het HLO biedt de mogelijkheid[10] om te bepalen wat specifiek en generiek is. Deze aanpak betekent dat Defensie alleen zelf ontwikkelt binnen het specifieke deel.
3. Met generieke componenten kan sneller het nieuwe IT-domein van de krijgsmacht worden ingericht. Dat bouwt sneller en zekerder omdat deze componenten zijn gelouterd door de tijd en minder fouten kennen. Door het HLO leidend te verklaren wordt voorkomen dat in het nieuwe domein de "huidige situatie" vanzelfsprekend wordt geautomatiseerd. Met het HLO

---

[10] Een gangbare norm die gebruikt wordt om het streef aantal applicaties te bepalen is de verhouding tussen het aantal gebruikers en het aantal applicaties. In 2014 staat het markt gemiddelde op 100 gebruikers per applicatie . Application rationalisatie ratio's (2013/2014), voor grote organisaties, (bron QA Services) gaan uit van deze norm. Gegevens van het Ministerie van Defensie Australië zijn gebaseerd op de doelstellingen uit het rapport Strategic Reform Program, 2009 en gaat eveneens uit van deze norm (circa 1000 applicaties voor 100.000 gebruikers)..

Voor het Ministerie van Defensie betekent dit dat het streefgetal voor het applicatielandschap circa 500 is, uitgaande van 50.000 gebruikers.

slaat Defensie nieuwe wegen in. Hierdoor ontstaat een beheersbaar en flexibel IT-domein dat veel meer doet dan *keeping-the-lights-on*.

4. Werken onder gemeenschappelijke architectuur: Onder regie van de HDBV/CIO wordt strikt gewerkt op basis van een eenduidige architectuur over alle ketens en in alle gebruikersomstandigheden om gezamenlijk naar dezelfde stip op de horizon te werken. De HDBV/CIO bewaakt dat zoveel mogelijk uniformiteit wordt gerealiseerd zonder de specifieke aspecten van de expeditionaire gebruiksomstandigheden uit het oog te verliezen. De stip op de horizon mag verschuiven, maar dan wel voor iedereen in dezelfde mate en richting.

5.3 Migratie

1. Het JIVC hanteert op basis van de kaders van de HDBV/CIO een rationalisatie methodiek om het bestand aan applicaties reeds op de bestaande infrastructuur te saneren. Daarnaast wordt deze methodiek gebruikt om te bepalen welke IT-toepassingen migreren naar de nieuwe IT-infrastructuur. Bestaande delen van de IT welke niet migreren naar de nieuwe groeikern faseren op zo kort mogelijke termijn uit. De rationalisatie methodiek kent vier mogelijke uitkomsten voor een applicatie:
   a. *FREEZE* (IT-toepassingen, tot moment uitfaseren, in de huidige vorm handhaven in de huidige IT-infrastructuur).
   b. *KILL* (met voorrang uitfaseren omdat het technisch of economisch niet rendabel is dit systeem in stand te houden).
   c. *ELU* (een *End-Life Update* geven en de levenscyclus in de *legacy* omgeving laten aflopen). Per uitkomst wordt er ook een *rollback* scenario opgesteld.
   d. *MIGRATE* (als *workload* gevirtualiseerd overbrengen naar de nieuwe IT-infrastructuur),
   e. *REBUILD* (vergelijkbare functionaliteit *cloud based* opnieuw inrichten).

   Een optie is om externen in te schakelen om de rationalisatie met een zo hoog mogelijke prioriteit uit te voeren.
2. Bij de sanering kan het definiëren van ontkoppelpunten en het vereenvoudigen van de processen leiden tot de afweging om *legacy* langer te gebruiken door deze als het ware "in te pakken". Met het inpakken worden alleen die zaken gebruikt die strikt noodzakelijk zijn. De toepassing draait dan als het ware als "een fabriek waar het licht uit is." Dit geeft tijd om de principes van de nieuwe manier van werken en IT-architectuur goed in te richten.

5.4 Rol van de nieuwe infrastructuur

De rol van de nieuwe infrastructuur is een "landingsbaan" voor de nieuwe toepassingen en geselecteerde toepassingen uit de huidige structuur en het bieden van een vernieuwd netwerk, werkplek en telecommunicatie faciliteiten. De nieuwe infrastructuur geeft invulling aan:

- Statische LGI en HGI infrastructuren.
- *Deployed* (OMUT) infrastructuren voor de diverse gebruikersomstandigheden.
- Innovatie projecten, zoals proefruimtes en gedecompartimenteerde (DMZ) infrastructuren voor de vernieuwing van de IT voor Defensie.
- Integratie van IT-toepassingen.

5.5 Innovatie en veranderbaarheid

1. Het HLO is als architectuur zoveel als mogelijk ontkoppeld van de organisatorische verbijzondering. Dit betekent dat mogelijke aanpassingen van de organisatie niet onmiddellijk leiden tot verandering van de totale architectuur inclusief het applicatielandschap en de infrastructuur. Het is de uitdaging om in de komende jaren de juiste ontkoppelpunten verder te expliciteren in zowel de processen als de output van de krijgsmacht. Daarmee ontstaat een toekomstbestendige en flexibele IT-ondersteuning.

2. De nieuwe IT wordt opgezet op basis van bouwstenen en kent daardoor een modulaire opbouw, waardoor de flexibiliteit en veranderbaarheid hoog is.
3. De IT-toepassingen worden zoveel als mogelijk onzichtbaar voor de gebruikers. Niet de toepassingen maar de informatiebehoefte komt centraal te staan. De nieuwe IT bevat voorzieningen om IT uniform toegankelijk te maken, afgestemd op rol, taak of functie.
4. Medewerkers krijgen de middelen om IT optimaal te benutten in de vorm van een digitale uitrusting.
5. Nieuwe toepassingen worden direct op de nieuwe infrastructuur ontwikkeld (zoals het informatiegestuurde optreden [IGO] voor de KMAR en de moderne werkplekomgeving). De nieuwe infrastructuur vervult de rol van innovatie- en integratiedomein en beproevingsomgeving met twee invalshoeken:
   a. De nieuwe IT-infrastructuur is een innovatieplatform voor alle nieuwe services die bij verandertrajecten ontwikkeld worden. Al deze nieuwe services blijven tot einde van de levenscyclus op de nieuwe IT-infrastructuur;
   b. De nieuwe IT-infrastructuur verhoogt de veranderbaarheid van de bestaande IT-toepassingen.
6. Defensie ontwikkelt in principe niet zelf. Defensie maakt bij nieuwe trajecten maximaal gebruik van reeds bestaande services uit de markt, Rijk of NATO. Ontwerp, bouw, migratie en beheer worden daarbij volgens DevOps principes gedaan. Dit houdt in dat in kleine teams gewerkt wordt die zowel rekening houden met beheer als het realiseren van functionaliteiten . De kracht van projectmatig werken (resultaatgericht) en beheerst beheer (stabiliteit, efficiëntie) worden zo gecombineerd.

5.6 Beveiliging als integraal onderdeel van de migratie

De toenemende behoefte aan samenwerking vereist meer koppelingen terwijl de cyberdreigingen toenemen. Om de informatiebeveiliging te blijven borgen vereist dit het continue blijven ontwikkelen en verbeteren van de beveiligingsmaatregelen zodat koppelingen met derden mogelijk blijven en functioneel kunnen verbeteren, terwijl risico's inzichtelijk en beheersbaar zijn.

5.7 Incrementele programmatische veranderingen

Veranderingen worden uitgevoerd in incrementele stappen van zes weken tot drie maanden. Veranderingen zijn onderdeel van een programma, spelen in op de veranderende behoeften van Defensie en houden rekening met onzekerheden in plaats van een *fixed price*, *fixed date*, *fixed result* benadering.

6. Samenwerking met de markt

6.1 Inleiding

Om de hiervoor genoemde doelstellingen goed door te kunnen voeren is het essentieel dat Defensie de markt betrekt bij de uitvoering van haar IT-dienstverlening. Dit kan Defensie het beste doen in een samenwerkingsmodel met de markt.

Dit hoofdstuk geeft uitwerking aan dit samenwerkingsmodel. Allereerst worden de uitgangspunten behandeld. Vervolgens wordt ingegaan op de te bereiken doelstellingen met de samenwerking. Er wordt afgesloten met de beveiligingseisen die worden gesteld aan beveiligen.

6.2 Uitgangspunten samenwerking

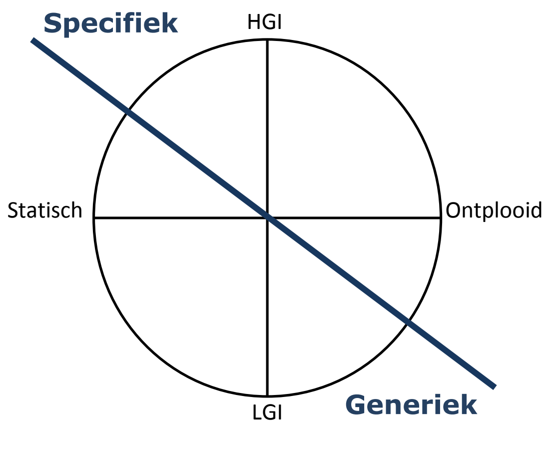
6.2.1 Samenwerking met de markt is noodzakelijk

In het rapport 'Grensverleggende IT' is geconcludeerd dat Defensie de markt nodig heeft om haar IT diensten te kunnen leveren. De wijze waarop Defensie dit doet, wordt 'Sourcing' genoemd. Sourcing betekent het (opnieuw) organiseren van processen, mensen en middelen in en tussen organisaties. Het gaat hier om het keuzeproces dat leidt tot varianten als zelf doen, samenwerken en uitbesteden. Wanneer wordt samengewerkt met de markt of diensten worden uitbesteed dan zal Defensie dit altijd moeten aanbesteden middels een geëigende (Europese) aanbestedingsprocedure.

Tegelijkertijd is de constatering dat Defensie altijd IT activiteiten onder eigen verantwoordelijkheid zal doen vanwege haar unieke primaire taak. Hierdoor ontstaat het samenwerkingsmodel, dat het beste kan worden omschreven als een samenwerking met de markt.

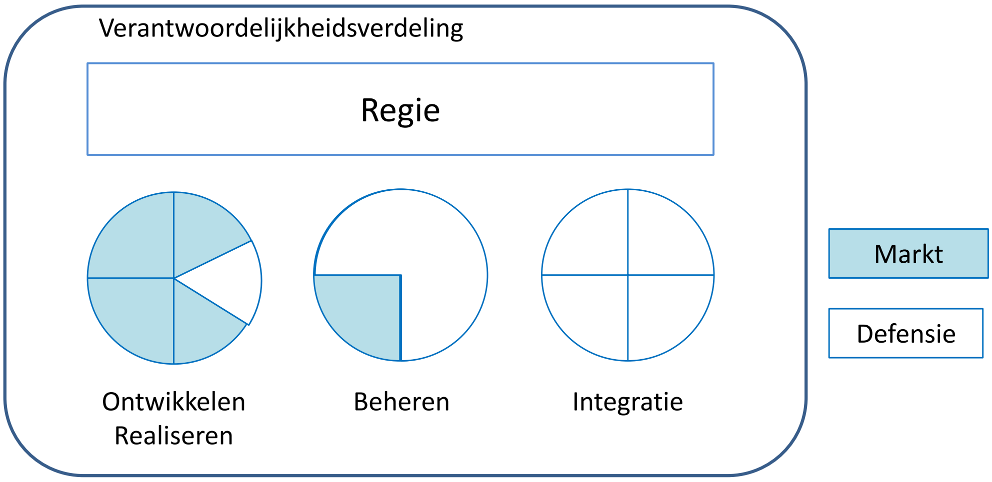
De generieke karakteristieken van dit model zijn onderstaand beschreven. Afwijkingen op deze karakteristieken per service zijn mogelijk, maar worden apart gespecificeerd:

- De strategische samenwerking van Defensie betreft de nieuwe IT. Hierbij worden conform het rapport 'Grensverleggende IT' alsmede het HLO de IT activiteiten langs de assen Statisch-Ontplooid en LGI-HGI ingedeeld (zie figuur hiernaast). Er is – als "derde as" – echter ook een scheidslijn tussen generieke IT en specifieke IT. IT welke gangbaar is in de markt wordt generieke IT genoemd. De specifieke IT betreft IT die bijzonder is voor Defensie (o.a. systemen voor commandovoering). Door de consolidatie van business effecten in het HLO is verbijzondering naar militair optreden niet uitgewerkt. Het is noodzakelijk om de huidige set van business effecten te verbijzonderen naar de capabilities voor het militair optreden ten aanzien van verschillende omstandigheden en de eisen die dit stelt aan de specifieke IT.



- Defensie kiest voor meerdere spartijen (best of breed) voor de nieuwe IT welke niet alleen worden geselecteerd op basis van prijs/prestatie, maar ook op basis van 'cultural fit' en perspectief voor medewerkers.
- De samenwerking vindt niet plaats in een aparte juridische entiteit.

- De samenwerking met de markt geschiedt gefaseerd in behapbare delen die voldoende groot zijn voor marktpartijen, marktconform en beheersbaar waarbij rekening wordt gehouden met het absorptievermogen van de uitvoeringsorganisatie. Hierbij wordt vooralsnog de indeling van services uit bijlage 1 gehanteerd.
- De huidige IT-infrastructuur blijft nog een aantal jaar operationeel onder verantwoordelijkheid van Defensie; hierbij kunnen externe partijen worden ingezet zoals nu ook al het geval is.
- Defensie behoudt zelf de regie en integratie11 functie (inclusief technische expertise) en laat zich hierbij ondersteunen door een externe strategische partner.
- De samenwerkingsaanpak brengt met zich mee dat Defensie de (integrale) eindverantwoordelijkheid houdt over de IT-infrastructuur.
- De verantwoordelijkheidsverdeling is conform het rapport 'Grensverleggende IT' als volgt bepaald (de uitvoering van activiteiten kan anders worden belegd), zie onder.



Samenwerken met de markt lukt alleen wanneer er een duidelijke verantwoordelijkheidsverdeling is. Wanneer die ontbreekt of onduidelijk is dan zal de opdrachtgever vrijwel altijd de volledige verantwoordelijkheid dragen. Daarom is bij de verantwoordelijkheidsverdeling gekozen voor het volgende:

Verantwoordelijkheid voor	Ontwikkelen & Realiseren	Beheren	Integreren (regie)
HGI	Markt/Defensie*	Defensie	Defensie
LGI – statisch	Markt	Markt	Defensie
LGI – ontplooid	Markt/Defensie	Defensie	Defensie

*: voor een bepaald deel zal gelden dat Defensie verantwoordelijk is.

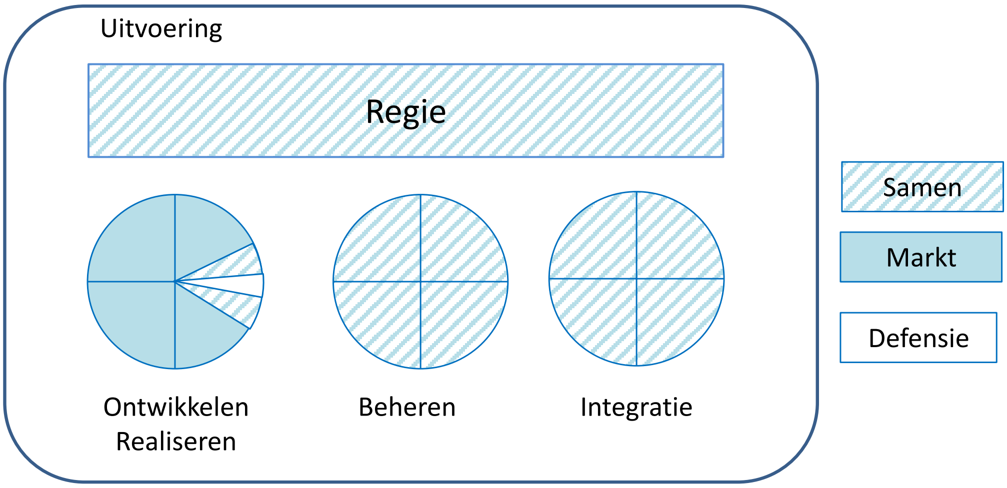
De exacte inhoud van de "taartpunten" (de IT objecten en IT activiteiten) worden bepaald door middel van de vijf scope criteria zoals in het HLO zijn beschreven. De criteria hebben

11 Technische integratie van diensten wordt zoveel mogelijk bij externe partij belegd. Technische integratie van wapensystemen wordt bij Defensie belegd.

alleen betrekking op nieuwe en gemigreerde IT-diensten. Het uitgangspunt is dat alle objecten en/of activiteiten qua verantwoordelijkheid aan de markt zijn over te dragen, tenzij één van de volgende uitspraken "waar" is (zie bijlage 2):

1. Het object of de activiteit is niet *overdraagbaar*.
2. De activiteit betreft instandhouding van een *hoog gerubriceerd* object.
3. De activiteit wordt uitgevoerd onder *ontplooide omstandigheden*.
4. De activiteit betreft *essentiële regievoering*.
5. Het is een *erkende uitzondering*.

- Binnen de verantwoordelijkheidsverdeling worden activiteiten door de externe partijen en Defensie gezamenlijk uitgevoerd binnen de regels en kaders van de verantwoordelijke. In onderstaand model is de samenwerking v.w.b. de uitvoering vorm gegeven. De condities waaronder deze inzet plaats vindt moet nader worden uitgewerkt. Defensiepersoneel blijft bij Defensie, maar wordt ingezet, voor zover nodig, bij IT-activiteiten die onder verantwoordelijkheid van de markt worden gebracht. Voor een klein specifiek deel zal gelden dat Defensie zelf ontwikkelt en realiseert.



- Eigenaarschap middelen (hardware en software) is belegd bij de markt (in ieder geval voor LGI, voor HGI moet dit nader worden uitgezocht). Sommige software contracten kunnen niet worden overgedragen. Terugname mogelijkheid moet gegarandeerd zijn.
- Het Wide Area Netwerk (WAN12) is van vitaal belang voor de bedrijfsvoering van Defensie13. Defensie hanteert voor het WAN specifieke ontwerpprincipes, zoals een sterk beveiligd koppelvlak (genaamd IEGI) naar externe netwerken. Vanwege het specifieke karakter en aanmerking als vitale infrastructuur blijft het WAN binnen Defensie en is

12 Onder het WAN wordt verstaan het NAFIN (glasvezelnetwerk van Defensie) inclusief de netwerklagen die daarop zijn gerealiseerd (tot aan het koppelvlak met de bekabeling in gebouwen). Dit is inclusief de huurlijnen die worden gebruikt voor het koppelen van locaties waar geen NAFIN is.

13 Het WAN is niet alleen vitaal voor de bedrijfsvoering van Defensie, maar is door een besluit van de staatssecretaris van Economische Zaken op 14 januari 2008 (nr. ET/TM/7135438) op grond van artikel 5.16 van de Telecommunicatiewet ook aangewezen als elektronisch communicatienetwerk dat geheel of hoofdzakelijk gebruikt wordt voor vitale overheidstaken.

samenwerking met andere partijen binnen de Rijksoverheid het best passend voor een strategische asset als het WAN.

- De externe partij investeert in de nieuwe IT-infrastructuur (voorfinanciering). De kosten van de voorfinanciering worden opgenomen in de tarieven van de dienstverlening. Betaling van deze partijen vindt plaats op basis van afgesproken prestaties per dienstverlening.
- De Samenwerkingsovereenkomst moet voldoende flexibiliteit bezitten om toekomstige dienstverlening (groeikern) te kunnen absorberen. Defensie neemt op basis van behoefte in de tijd diensten af (flexibiliteit) op basis van nadere overeenkomsten binnen de samenwerkingsovereenkomst.
- Het stimuleren van de innovatie bij en door externe partijen moet een bewust onderdeel zijn van de samenwerking. Dit wordt o.a. ingevuld door middel van:
  - Spanning tussen continuïteit en innovatie wordt niet in het contract ondergebracht. Benoem innovatie apart met een separate geldstroom.
  - Behoud mogelijkheden om binnen Defensie naar eigen keuze en eigen wensen innovatieve initiatieven te ontplooien met derden.
  - Reserveer innovatiebudget, met bij aanwending financiële middelen afspraken over *time to market*.
- De vastgestelde beveiligingseisen moeten in overeenstemming met de Defensiewet worden toegepast. Voor vitale infrastructuur kan het noodzakelijk zijn om gebruik te maken van de uitzonderingsbepalingen in de Defensiewet.
- Defensie moet de mogelijkheid hebben om in een 'last resort' situatie haar IT zelf te kunnen beheren. Daartoe kan Defensie ten allen tijde de dienstverlening van de markt terug nemen, de voorwaarden en condities waaronder dit gebeurt, moeten worden uitgewerkt.

6.2.2 *Personeel heeft perspectief*

Het personeel wordt binnen dit scenario niet naar buiten geplaatst. Echter wanneer de transitie naar de nieuwe IT wordt uitgevoerd conform het HLO dan zal dit consequenties hebben voor het personeel. De marktervaringen met nieuwe IT leidt tot een beperktere inzet van personeel maar tegelijkertijd ook tot de behoefte aan andere skills.

Dit heeft consequenties voor de inrichting van de IT-keten binnen Defensie en het benodigde aantal medewerkers en de kennis/kunde en competenties van het personeel. Daarom is het belangrijk om voldoende perspectief voor het huidige personeel te houden. Binnen het de constructie van samenwerken met de markt heeft het personeel perspectief in de vorm van o.a.:

- Beheren van HGI zal altijd door Defensie worden uitgevoerd.
- Beheren van huidige omgeving zal nog enige jaren voortduren.
- Samen beheren van nieuwe omgeving LGI met externe partij.
- Regie is cruciale rol die bij Defensie blijft.

6.2.3 *Regie is cruciaal voor een succesvolle samenwerking*

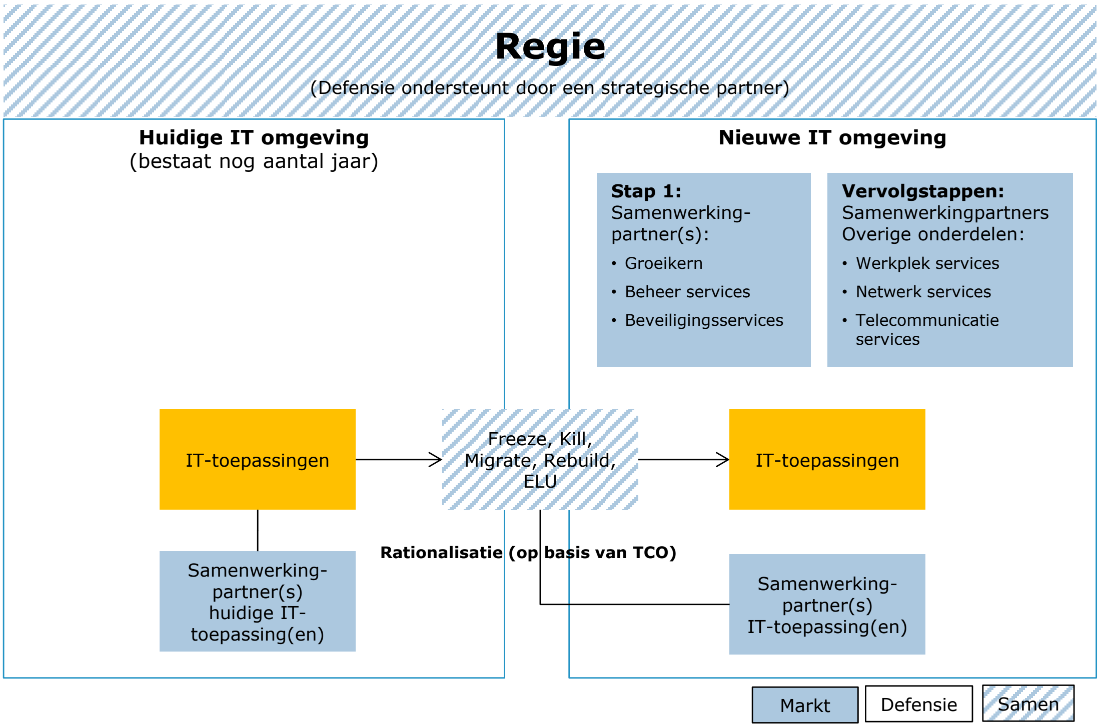
Regie is essentieel bij de vernieuwing en modernisering. Aansturing van leveranciers, coördinatie en sturing van de migratie-activiteiten en specificeren wat verwacht wordt van externe partijen is essentieel. Tevens dient er aandacht te zijn voor monitoring, review en audit mogelijkheden (rapport Elias).

Als onderdeel van de IT regie moet de IT strategie, Enterprise architectuur (met als basis het HLO) en governance verder worden ontwikkeld door de HDBV. Daarnaast moet op uitvoerend niveau door de DMO meerdere externe partijen worden aangestuurd in combinatie met een deel van de dienstverlening die door Defensie zelf wordt uitgevoerd. CDS is hierbij verantwoordelijk voor het in balans brengen van de behoeftes, middelen en de beschikbare capaciteit met Projecten Portfolio Management (PPM) als instrument. Binnen dit hele spectrum is het aanbrengen en bewaken van de integraliteit noodzakelijk.

Het versnellen en versterken van regie door ondersteuning van een externe strategische partner wordt daarom als cruciale succesfactor gezien. Hierbij gelden de volgende uitgangspunten:

- Defensie blijft zelf "de" regieorganisatie
- Externe strategische partner versterkt Defensie in haar rol
- De scope van de strategisch partner is:
    - Uitwerken HLO.
    - Advisering bij migratie IT-toepassingen.
    - Advisering opzet en samenwerking met de markt.
    - Advisering bij continuïteit van de huidige omgeving.
    - Quality Assurance en Risk Management.
    - Ondersteunen bij doorontwikkelen en professionaliseren regieorganisatie.
    - Inregelen integratie.
- De externe strategische partner kan / mag niet in de uitvoering zitten.

Dit wordt in onderstaand figuur verduidelijkt.



6.3 Doelstellingen samenwerking IT

In samenwerking met de markt worden voor de IT-dienstverlening de volgende doelstellingen na-gestreefd:

Doel	Subdoel	Doelstelling
Kwaliteit dienstverlening	Garanderen continuïteit en beschikbaarheid	Defensie verwacht, zowel gedurende de overgang van de dienstverlening als in de operationele fase, dat de externe leverancier het garanderen van continuïteit en beschikbaarheid van de dienstverlening aan eindgebruikers als hoogste prioriteit heeft.
	Voldoen aan alle geldende beveiligingseisen	Voor Defensie is beveiliging, naast continuïteit, de belangrijkste pijler waaraan IT moet voldoen. De externe leverancier borgt dat zijn volledige dienstverlening aan Defensie altijd voldoet aan de geldende beveiligingseisen.
	Verbeteren van het innovatievermogen	Van de externe leverancier wordt verwacht dat hij vanuit zijn kennis en ervaring met innovatieve oplossingen komt zodat de IT van Defensie actueel blijft en van de nieuwste technologieën kan profiteren.
	Bijdragen aan vermindering complexiteit	Defensie verwacht van de externe leverancier dat deze bijdraagt aan een vermindering van de complexiteit van de IT, zowel met betrekking tot de infrastructuur als het applicatielandschap.
Kwaliteit partner	Loopbaanperspectief Defensiepersoneel	Van de externe leverancier wordt verwacht dat hij een positieve bijdrage levert aan het loopbaanperspectief van medewerkers van Defensie door middel van opleiding, stages en job rotation.
Besturing en beheersing van de kosten van de dienstverlening	Flexibiliteit	De dienstverlening moet kunnen meebewegen met de vraag naar diensten.
	Vermindering administratieve lasten	De externe leverancier draagt zorg voor vereenvoudiging van regieprocedures en draagt bij aan de professionalisering van de IT-regie.
	Kostenvermindering door efficiency verbetering	De externe leverancier zorgt voor een structurele kostenverlaging door zijn professionaliteit, marktkennis en schaalgrootte.

Tabel 1. Doelstellingen samenwerking met de markt

6.4 Beveiligingseisen

Op de IT infrastructuur van Defensie draaien belangrijke informatiesystemen voor de bedrijfsvoering. Wanneer de informatie uit deze systemen in verkeerde handen komt, ontstaat een substantieel risico voor de staatsveiligheid. Wanneer bijvoorbeeld logistieke systemen niet beschikbaar zijn, dan kunnen logistieke ketens stagneren tot in het operatiegebied. Daarnaast bevatten deze systemen bijvoorbeeld de munitievoorraad van Defensie zowel in Nederland als in het operatiegebied. Hieruit valt de slagkracht van uitgezonden eenheden af te leiden en ook de exacte vindplaats in de complexen van Defensie. De eisen die hieronder staan opgesomd, gaan uit van één geheel aan IT-diensten (in casu de meest zware variant). De eisen die gesteld worden aan samenwerking van het gehele IT-diensten, zijn:

1. Gezien de staatsgeheime rubricering en het vitale karakter van de IT-diensten dient het ABDO te worden bedongen bij de verwerving.
2. Alleen functionarissen met een Nederlandse nationaliteit mogen geplaatst worden op een vertrouwensfunctie. Daarnaast dient bij vertrouwensfuncties de af te geven Verklaring Geen Bezwaar (VGB) te corresponderen met de zwaarte ervan, waarbij voor beheerders die beschikken over volledige rechten op (technische) omgevingen een VGB op niveau B vereist is.
3. De AIVD en/of MIVD moet een VGB hebben afgegeven alvorens personeel met staatgeheim gerubriceerde defensiegegevens in aanraking komt.
4. Voor alle functies waarbij kennisname van staatsgeheimen en/of gemerkte informatie niet noodzakelijk is, is een Verklaring Omtrent het Gedrag (VOG) en een Geheimhoudingsverklaring een vereiste.
5. De dienstverlening moet door een Nederlandse rechtspersoon worden uitgevoerd.
6. De dienstverlening moet door een vaste Nederlandse vestiging worden uitgevoerd.
7. De dienstverlening (informatie, programmatuur, apparatuur en personeel) voor de IT-diensten dient plaats te vinden op Nederlands grondgebied.
8. Een datacenter dient op Nederlands grondgebied te staan vanwege de noodzaak militaire interventie uit te kunnen voeren.
9. Defensie dient een exit clausule op te nemen in het contract met de leverancier die gebaseerd is op een exit strategie in het geval de leverancier wordt overgenomen door een ongewenste partij.
10. Netwerkdetectie op het netwerk van de dienstverlener door DefCERT is een randvoorwaarde.
11. Op de koppeling tussen de ontwikkelomgeving en de IT-omgeving (productieomgeving) zijn de normen van een koppeling tussen Defensie en een commerciële partij, voor beide omgevingen van toepassing.
12. De vervlechting van de informatie op MULAN maakt het in de meeste gevallen niet mogelijk om delen van de dienst te ontvlechten en daarmee te onderwerpen aan een lager beveiligingsregime.

Met het stellen van bovengenoemde maatregelen kan de samenwerking van de IT van Defensie op een dusdanige wijze plaatsvinden dat de veiligheidsrisico's op een voldoende wijze worden gemiti-

geerd. Deze beveiligingseisen zijn door de SG vastgesteld en vastgelegd in (referte M) in de Bestuursraad van 23 januari 2015.

7. Samenvatting en conclusies

7.1 Samengevat

IT is voor Defensie cruciaal. Defensie is in toenemende mate afhankelijk van IT bij het uitvoeren en ondersteunen van missies, oefeningen en het uitvoeren van nationale taken. In de loop van 2014 is vastgesteld dat de IT kwetsbaar is waardoor Defensie risico's loopt op het gebied van beveiliging en continuïteit. Vooral de technische staat van de IT-infrastructuur is daarvan de oorzaak.

De technische modernisering van de IT-infrastructuur heft niet alleen knelpunten op die betrekking hebben op beveiliging en continuïteit, maar opent tegelijkertijd de weg naar innovatie en flexibilisering van de IT als geheel om daarmee invulling te geven aan de rol die IT in de toekomst voor Defensie dient te vervullen. De toekomstige rol van IT is het optimaal ondersteunen van de beoogde business effecten en de business eisen zoals deze eind 2014 zijn geïnventariseerd door CDS en HDBV, namelijk:

- Business en mens staan centraal, IT sluit aan.
- De IT maakt veilig samenwerken in wisselende verbanden mogelijk.
- IT is betrouwbaar en beschikbaar.
- Met IT is Defensie *wereldwijd connected.*
- De IT is geschikt voor verwerken, opslaan en analyseren voor zeer grote hoeveelheden informatie.
- De IT is eenvoudig en snel aanpasbaar.

Deze eisen staan niet op zichzelf. Deze worden ingegeven door overkoepelende trends in de informatiemaatschappij, de Defensie-industrie en de behoeften om netwerkend op te treden. Ook voldoet de IT van de toekomst aan de pijlers continuïteit, beveiliging en innovatie conform de visie "Let's make IT happen".

Het realiseren van moderne IT die voldoet aan de eisen van de toekomst vraagt om verschillende ingrepen. Enerzijds is technische modernisering nodig van de IT-infrastructuur anderzijds is het ook noodzakelijk het complexe geheel van IT-toepassingen (applicaties) aan te pakken. Het huidige geheel van IT-toepassingen kenmerkt zich door grote diversiteit in technologie, sterk uiteenlopende levenscyclus van IT-toepassingen (mix van moderne en verouderde toepassingen) en gebrek aan veranderbaarheid (inflexibel).

7.2 Conclusies

De huidige staat van de IT van Defensie is verouderd en sluit niet aan bij de behoeften van een moderne krijgsmacht. De oorzaken hiervoor zijn:

- De technische IT-infrastructuur bevat kwetsbaarheden. Er is onvoldoende reservecapaciteit beschikbaar om adequaat op uitval te reageren en delen zijn verouderd. Dat kan de continuïteit van de operationele inzet en de bedrijfsvoering in gevaar brengen. Daarom moet de IT-infrastructuur met voortvarendheid gemoderniseerd worden.
- Het huidige landschap van IT-toepassingen is een lappendeken met vele verschillende toepassingen die geen logisch geheel vormen. Medewerkers die informatie nodig hebben en de netwerkbenadering worden onvoldoende ondersteund. De noodzakelijke modernisering van de IT-infrastructuur opent mogelijkheden om ook het complexe landschap van IT-toepassingen (applicaties) geschikt te maken voor de behoeften van een moderne krijgsmacht.

7.3 Principes van het High Level IT-ontwerp (HLO)

Het High Level IT-ontwerp heeft de volgende kenmerken:

- De gemoderniseerde IT (zowel de infrastructuur als de toepassingen) moet flexibel en snel veranderbaar zijn. Deze omgeving wordt opgezet op basis van bouwstenen, is modulair van opbouw en daarmee flexibel en veranderbaar. Het HLO is als architectuur zoveel als mogelijk ontkoppeld van de organisatorische verbijzondering. Eventuele aanpassingen van de organisatie leiden daarmee niet onmiddellijk tot verandering van de totale architectuur inclusief het applicatielandschap en de infrastructuur.
- De IT-toepassingen worden zoveel als mogelijk onzichtbaar voor de gebruikers. Niet de toepassingen maar de informatiebehoefte komt centraal te staan. De nieuwe IT bevat voorzieningen om IT uniform toegankelijk te maken, afgestemd op rol, taak of functie. Medewerkers krijgen de middelen om IT optimaal te benutten in de vorm van een digitale uitrusting.
- Om informatiedominantie te behouden moet Defensie in staat zijn voortdurend te innoveren en te experimenteren. De gemoderniseerde IT moet de basis leggen voor een innovatie- en beproevingsdomein waarmee Defensie continu nieuwe ontwikkelingen kan volgen.
- De gemoderniseerde IT is een groeikern en vervangt niet in één keer de huidige IT-infrastructuur en alle IT-toepassingen. De groeikern zal in fasen de bestaande IT overnemen. De bestaande IT blijft gedurende deze verandering in gebruik om de processen binnen Defensie te ondersteunen (tot en met de operationele inzet).
- Er komt een nieuwe IT-infrastructuur naast de oude. De huidigeIT-infrastructuur blijft zo kort mogelijk beschikbaar, maar zolang als nodig en daarop zullen de vereiste IT-toepassingen regulier beschikbaar zijn. De nieuwe infrastructuur kenmerkt zich door een opzet als groeikern, die meegroeit met de behoeften van Defensie.
- De nieuwe IT wordt opgezet op basis van bouwstenen en kent daardoor een modulaire opbouw, waardoor veranderbaarheid hoog is.
- Defensie ontwikkelt in principe niet zelf. Echter, op een beperkt aantal terreinen ontwikkelt Defensie bewust zelf.
- De toenemende behoefte aan samenwerking vereist meer koppelingen terwijl de cyberdreigingen toenemen. Om de informatiebeveiliging te blijven borgen vereist dit het continue blijven ontwikkelen en verbeteren van de beveiligingsmaatregelen zodat koppelingen met derden mogelijk blijven en functioneel kunnen verbeteren, terwijl risico’s inzichtelijk en beheersbaar zijn.

Bijlage 1: Refertes

1. Visie Grensverleggende IV/ICT, Lets make IT happen!, versie 2.1 definitief
2. Op weg naar grensverleggende IV/ICT Defensie, *Actieplan voor het op orde brengen van de IV/ICT Defensie, v*ersie 4.0 definitief
3. Strategische Visie op de Netwerk en Informatie Infrastructuur, versie 1.0
4. Nota – Participatie NAVO *Federated Mission Network*, BS/201419526, 14 augustus 2014

Bijlage 2: Specifieke elementen bij samenwerking met de markt

Verdeling verantwoordelijkheid Markt-Defensie

De samenwerking is gericht op het uitvoeren van **nieuwe en gemigreerde** IT-diensten. De scope welke activiteiten in aanmerking komen om qua verantwoordelijkheid aan de markt over te dragen wordt feitelijk bepaald door de kenmerken die op de uit te voeren activiteiten (of verantwoordelijkheden) voor specifieke objecten van toepassing zijn. Het uitgangspunt is dat alle objecten en/of activiteiten qua verantwoordelijkheid aan de markt over gedragen kunnen worden, tenzij één van de volgende uitspraken "waar" is:

1. Het object of de activiteit is niet *overdraagbaar*.
2. De activiteit betreft instandhouding van een *hoog gerubriceerd* object.
3. De activiteit wordt uitgevoerd onder ontplooide *omstandigheden*.
4. De activiteit betreft *essentiële regievoering*.
5. Het is een *erkende uitzondering*.

De uitwerking van deze criteria is als volgt:

1. Overdraagbaarheid

Dit criterium is bedoeld om objecten en/of activiteiten, die een technisch of juridisch onlosmakelijk onderdeel zijn van een groter (niet-IT-) geheel, uit te filteren en daarmee buiten de scope te plaatsen. Er zijn drie manieren om "onlosmakelijk" verbonden te zijn.

Technisch niet-overdraagbaar	Een object of activiteit is niet overdraagbaar als het een technisch onlosmakelijk onderdeel is van een niet-IT-geheel. Veelal is het object of activiteit ook als één geheel verworven. Meestal worden 'voorzien in' activiteiten uitgevoerd door de leverancier (of zijn/haar toeleveranciers) van het niet-IT-object.
Contractueel niet-overdraagbaar	Een object of activiteit is niet-overdraagbaar als de juridische overeenkomst blijvend verhindert dat het object of activiteiten worden overgedragen aan de Opdrachtnemer (samenwerking). Of dat er geen overeenkomst, na beeindiging van de oorspronkelijke, is af te sluiten met soortgelijke functionaliteit.
Militaire capaciteit	Objecten en activiteiten die onlosmakelijk onderdeel zijn van gedefinieerde wapensystemen. Het object of de activiteit heeft een direct gevolg op of is een onderdeel van het militaire vermogen van Defensie. Het object of de activiteit heeft een directe relatie met doelen of opdrachten en zal concreet benoemd moeten worden.

2. Instandhouding van een hoog gerubriceerd object

Dit criterium spreekt van activiteiten voor de instandhouding van hoog gerubriceerde objecten. Er wordt alleen over instandhouding gesproken omdat ontwerpen c.q. bouwen van hoog gerubriceerde objecten ook *commercial of the shelf* kan worden aangekocht (bijvoorbeeld wapensystemen). Hieronder is instandhouding naast voorzien in en afstoten toegelicht.

	Hoog gerubriceerd (HGI)	Laag gerubriceerd (LGI)
Beheren	Defensie	Markt
Ontwerp en Bouw	Markt(bij uitzondering ook Defensie)	Markt

De vraag of een object hoog gerubriceerd is, wordt vanuit de bestaande formele rubriceringssystemen beantwoord. Vijf formele rubriceringssystemen zijn hierbij relevant. Onderstaande figuur geeft voor ieder van deze rubriceringssystemen aan wanneer een IT-object als hoog gerubriceerd geldt.

Rubriceringssysteem → niveau	***Hoog gerubriceerd***	***Laag gerubriceerd***
Nationale rubricering	• Stg ZEER GEHEIM • Stg GEHEIM	• Stg CONFIDENTIEEL • DEPARTEMENTAAL VERTROUWELIJK
NATO-rubricering	• COSMIC TOP SECRET • NATO SECRET	• NATO CONFIDENTIAL • NATO RESTRICTED • NATO UNCLASSIFIED
EU rubriceringen	• EU TOP SECRET • EU SECRET	• EU CONFIDENTIAL • EU RESTRICTED
Merking	•	• PERSONEELSVERTROU WELIJK • COMMERCIEEL VERTROUWELIJK • MEDISCH GEHEIM • INTERN BERAAD • INTERN GEBRUIK DEFENSIE
Politie	• Politie Zeer Geheim • Politie Geheim	• Politie Zeer Vertrouwelijk • Politie Vertrouwelijk / Politie Intern

3. Ontplooide (deployed, mobiel en uitgestegen) omstandigheden

Indien de activiteit (of een onlosmakelijk deel ervan) wordt uitgevoerd onder 'ontplooide omstandigheden', dan is zij buiten scope en niet-uitbesteedbaar. Samenvattend betekent dit het volgende

voor de diverse omstandigheden:

Omstandigheid	Voorbeeld	Markt / Defensie
Statisch	Nederland, kazernes, vliegbases, havens.	Markt
Deployed	Compound, schip (thuishaven)	Defensie
Mobiel	In voertuig, schip (varend)	Defensie
Uitgestegen	In de contactomgeving met mogelijk geweld	Defensie

4. Essentiële regievoering

De toepassing van het criterium is gebaseerd op een concreet overzicht van benoemde regie-activiteiten (c.q. verantwoordelijkheden), die essentieel voor de regievoering van Defensie zijn. Deze regie-activiteiten blijven achter bij Defensie en worden belegd in de lijnorganisatie (bijvoorbeeld VAM).

5. Erkende uitzondering

Het object is (of wordt) expliciet erkend als uitzondering en als zodanig met redenen opgenomen in het overzicht "Uitzonderingen samenwerking", dat als bijlage van het samenwerkingscontract gedurende de contractperiode wordt onderhouden.

Dit criterium is niet bedoeld als vrijbrief om uitzonderingen toe te laten en overeen te komen. Het idee is, dat de eerste vier criteria volstaan en dat de lijst met "erkende uitzonderingen" leeg is. Echter, Defensie gaat in het samenwerkingstraject voor een lange termijn een contract aan met leveranciers. Gedurende de looptijd van het contract kunnen opvattingen over de scope van de samenwerking veranderen bijvoorbeeld door nieuwe technologie. Het idee is dan steeds, dat objecten of activiteiten die tot "uitzondering" worden verheven aanleiding geven tot het opsporen van de "criteria achter de uitzonderingen". Op basis hiervan kunnen de criteria dusdanig worden aangepast c.q. verfijnd dat hiermee de uitzondering wordt gemitigeerd. Overigens houdt Defensie zich altijd het recht voor om dingen zelf te blijven doen.

Overige scope vraagstukken:

Wide Area Network: erkende uitzondering.

Een onderdeel van de scope omvat het *Wide Area Netwerk* (WAN) van Defensie. Dit is van vitaal belang voor de bedrijfsvoering van Defensie[14]. Onder het WAN wordt verstaan het NAFIN (glasvezelnetwerk van Defensie) inclusief de netwerklagen die daarop zijn gerealiseerd (tot aan het koppelvlak met de bekabeling in gebouwen). Dit is inclusief de huurlijnen die worden gebruikt voor het koppelen van locaties waar geen NAFIN is.

Defensie hanteert voor het WAN specifieke ontwerpprincipes, zoals een sterk beveiligd koppelvlak

14 Het WAN is niet alleen vitaal voor de bedrijfsvoering van Defensie, maar is door een besluit van de staatssecretaris van Economische Zaken op 14 januari 2008 (nr. ET/TM/7135438) op grond van artikel 5.16 van de Telecommunicatiewet ook aangewezen als elektronisch communicatienetwerk dat geheel of hoofdzakelijk gebruikt wordt voor vitale overheidstaken.

(genaamd IEGI) naar externe netwerken. Het loslaten van deze principes wordt bij samenwerking niet acceptabel geacht, gezien het vitale karakter van de WAN-dienstverlening.

De conclusie op basis van het bovenstaande is dat, vanwege het specifieke karakter en aanmerking als vitale infrastructuur, samenwerking met andere partijen binnen de Rijksoverheid het best passend is voor een strategische asset als het WAN. Hierbij worden de volgende argumenten als doorslaggevend gezien. De toepassing van het WAN strekt zich uit tot en met het operationele domein en is daarmee van vitaal belang voor de kerntaken van Defensie. Daarbij komt dat het WAN niet alleen door Defensie in het operationeel domein wordt gebruikt maar ook bijvoorbeeld door de Politie (C2000) en bondgenoten. Tot slot is reeds het maximale van het WAN aan marktpartijen uitbesteed, zie de eerdere opsomming bij de onderdelen van het WAN. Daarmee wordt het WAN buiten de scope van deze samenwerking IT geplaatst als erkende uitzondering. De huidige samenwerking met de markt (de bestaande contracten) worden gecontinueerd, terwijl de zeggenschap bij Defensie blijft.

Tweeden

Een ander vraagstuk binnen de scope betreft het verlenen van diverse IT-diensten aan andere Ministeries of aan daaronder ressorterende diensten binnen het Openbare Orde & Veiligheid domein (OOV) (hierna: "tweeden"). Op dit moment zijn dat de volgende diensten:

- Connectiviteit (dragerdiensten, > 40 VPN’s) t.b.v. BZK (Haagse Ring).
- Connectiviteit (dragerdiensten) t.b.v. V&J (C2000).
- Housing (fysiek datacentercapaciteit 1000 m^2) t.b.v. BZK (C2000).
- Housing (fysiek datacentercapaciteit 800 m^2) t.b.v. Justitie (Recentus).
- Applicatiehosting t.b.v. IND (Indis en Indigo).
- Werkplekhosting & dienstverlening t.b.v. IND (WIND: 2600 werkplekken).
- ICT Backoffice activiteiten t.b.v. AZ (inhuur mensen).
- ICT Backoffice CTIVD (inhuur mensen).

Het volume van de dienstverlening aan “tweeden” is in verhouding tot de totale IT-dienstverlening van Defensie relatief beperkt (ongeveer 10-15% van het financiële volume). De omvang van vooral de dienstverlening voor C2000 en de IND is relatief groot. De dienstverlening voor de Haagse Ring wordt door sommige marktpartijen als strategisch beschouwd. Wanneer WAN-dienstverlening wordt uitgesloten van de scope, dan gaan deze “tweeden” uiteraard ook niet mee in de samenwerking.

Het opnemen van de dienstverlening aan “tweeden” in de IT-infrastructuur kan als strijdig beschouwd worden met de kaders van de Defensiewet. Defensie moet daarom motiveren waarom de dienstverlening aan tweeden ook ziet als levering van gevoelige diensten of materieel. Waar dit niet het geval is moet geobjectiveerd worden waarom het toch als één geheel met de Defensie-dienstverlening (gemengde opdracht) wordt uitbesteed. Het opnemen van dienstverlening aan tweeden kan gezien worden als het onnodig samenvoegen van opdrachten (clusterverbod). Gemotiveerd moet worden waarom de dienstverlening niet in aparte percelen kan worden ondergebracht.

Tot slot kan in de samenwerking alleen een eventuele uitbreiding van de bestaande dienstverlening aan de orde zijn als het gaat om diensten voor de huidige tweeden.

Diensten voor “tweeden” waarbij geen sprake is van een hoge mate van technologische en organisatorische vervlechting met de IT-dienstverlening van Defensie (lees: waarbij beëindiging niet tot wezenlijke continuïteitsrisico's voor de dienstverlening leidt) kunnen niet worden betrokken in de

samenwerking en afgebouwd. Wanneer diensten niet worden uitbesteed dan kan deze dienstverlening blijvend worden gecontinueerd.